

السيبرانية

هاجس العصر

د. منى الأشقر جبور

المركز العربي للبحوث القانونية والقضائية



د. منى الأشقر جبور

جدول المحتويات



المقدمة
إطار الدراسة وأهدافها

١. إطار الدراسة

تندرج هذه الدراسة، في إطار جهود جامعة الدول العربية، التي أخذت على عاتقها، منذ سنوات عدة، مهمة نشر الوعي، على مستوى مراكز القرار العربي، بأهمية الأمن السيبراني، وبالحاجة إلى التعاون لتحقيقه، وذلك عبر تنظيمها ورعايتها، عددا من المؤتمرات، والمنشورات، واللقاءات، جمعت أكاديميين وخبراء، ونوقشت خلالها المسائل المتصلة به، من جوانبها كافة: الاجتماعية، الاقتصادية، القانونية، والتقنية. وعليه، فقد انطلقت هذه الدراسة من رؤية حددت معالمها عبر مقاربة لواقع الحال، ومتطلبات بناء الثقة، وارساء قواعد مرنة تسمح بمواكبة تحديات الاختراقات السيبرانية، والحد من الخسائر، التي تترتب عليها.

كما تندرج أيضا، في إطار الاهتمام الدولي المتصاعد بالأمن السيبراني، وما فرضه من تحولات طاولت الحياة اليومية للمواطن، بدءا من الممارسات الحكومية، مرورا بالعلاقات بين الدول، وصولا إلى جهود المنظمات الدولية والاقليمية، لاسيما منها الأمم المتحدة، والاتحاد الأوروبي، ودول الكمنولث، وجامعة الدول العربية، بمختلف اداراتها وهيئاتها،

فقد ترافق اعتماد الأفراد على تقنيات المعلومات والاتصالات، في انجاز مختلف أنشطتهم اليومية، من مهنية وشخصية، مع بروز عدد من التحديات، يأتي في مقدمها، طائفة من الحقوق التي لا بد من مراعاتها وتنظيمها، وتمكين المواطن من ممارستها، ضمن إطار يمنع الاعتداء عليها يضاف الى ذلك، كم من المخاطر يفرض اتقان الاستخدام الأمن لهذه التقنيات، واولها الانترنت. ولا يقف الامر عند حدود التقنيات التي يستخدمها، بل يتعداه إلى تلك التي لا يستخدمها، وانما يتأثر بها بشكل غير مباشر، نتيجة استخدام الآخرين لها. فالمؤسسات في القطاعين العام والخاص، تدير شؤونها، او شؤون المستفيدين من خدماتها، بالاعتماد على تقنيات المعلومات والاتصالات. والمثال البديهي الذي يساق هنا، هو سجلات المواطنين في الدوائر الرسمية، كالصحة، والاحوال الشخصية، والأمن، والمعاملات التجارية والمالية، وغيرها الكثير.

فالانترنت، والبث الفضائي، والهواتف الجوالة، قنوات مفتوحة للاتصال وللمشاركة، في المساحات العامة، التي خلقتها الوسائل الجديدة، والتي ما زالت تتسع وتتمدد بشكل مستمر، مع توسع الشرائح والفئات التي تطاولها، ودفق المعلومات وتنوعها. وبالفعل، فقد فتحت هذه التقنيات الباب واسعا امام الكثير من الخيارات، التي لم تكن متاحة سابقا. فالهواتف الذكية، والتي انتشرت بسرعة في الدول العربية، تستخدم لمتابعة الأمور المتعلقة بالعمل، كما تستخدم للحفاظ على الاتصال الدائم بالأسرة والأصدقاء، ولتبادل المعلومات، والدردشة، والمشاركة في كل تفاصيل الحياة تقريبا.

وانتقل المواطن إلى المشاركة في الحياة العامة، بوطنه، وبسواه، من خلال ابداء آرائه، ونشرها، والاطلاع على الاتجاهات العالمية، والاقليمية، والمحلية دون استثناء. فالمهارات المطلوبة لمستخدم الإنترنت، لا تتطلب كثيرا من الجهد، ولا تختلف عن تلك المهارات التي يحتاجها المهني الإعلامي أو السياسي، أو صاحب القرار. وغني عن القول، ما أوجده هذا الواقع من أزمة مفاجئة في تحديد المسؤوليات، على مستوى أخر، هو المستوى الإعلامي. فقد كاد كل مواطن يتحول إلى إعلامي، ومراسل، بينما الإطار التشريعي، في معظم الدول، ما زال الإطار الذي يحدد مسؤوليات المهنيين، في الإعلام التقليدي.

وينطبق هذا الامر على الادارات الحكومية، التي أنشأت قواعد بيانات، تضم معلومات هائلة عن المواطنين والمقيمين، لإدارة شؤونهم، وتسهيل وتقديم خدمات لهم، ذات جودة عالية، وبكلفة اقل، وتحسين علاقة المسؤول بالمواطن، وتوطيد الثقة بينهما. وقد لجأ العديد من الدول، إلى الاعتماد على "الحكومة الإلكترونية"، كأداة ناجعة للتحديث الاداري، وتسريع عجلة العمل، وملاقاة شروط الشفافية في إدارة الشأن العام، والمساءلة، والمرونة، والإدارة الرشيدة، وكذلك لمكافحة الهدر، ومحاربة الفساد.

وقد أسس الاعتماد على هذه التقنيات، لدفق هائل من المعلومات والبيانات التي تتوزع بين علنية من جهة، وسرية من جهة ثانية. وتتفاوت الدرجات بين ما هو سري، وحساس، وشديد الخطورة؛ ما طرح تحديات عديدة، ليس اقلها السهر على سلامة البيانات وأمنها، كما على أمن الأنظمة واستمرارية عملها، ومصداقيتها، تجاوبا مع المبادئ الادارية، التي تفرض، فيما تفرض، استمرارية المرفق العام بانتظام، ودون انقطاع، حفاظا على المصلحة العامة.

وعلى خط مواز، أسست البنية التحتية لتقنيات المعلومات والاتصالات، لحركة تدفق المعلومات عبر الحدود الجغرافية بين الدول، محولة العالم إلى "قرية كونية صغيرة"، ففرضت ثورة المعلومات التي أرستها، واقعا جديدا على السيادة الوطنية، الأمر الذي جعل الدولة تعاني من مشكلات أشد وأخطر، من تلك التي واجهتها من قبل. فالى مسائل الأمن على الحدود، ومسائل الأمن القومي التقليدية، برزت مشكلة السيادة على الفضاء السيبراني، وعلى العلاقات التي تحاك على الانترنت، بين أشخاص موجودين على أراض مختلفة، خاضعة لعدد من السيادات، حيث يختلف بلد مصدر العمل، وبلد تحقق نتائجه، والبلاد التي تمر عبرها البيانات. فالفضاء السيبراني، مكان مختلف، لكنه شديد الارتباط بالعالم المادي، وليس مستقلا عنه، كما اعلن بارلو في شرعة استقلال الانترنت، التي انتشرت بشكل واسع منذ العام ١٩٩٦[1].

فالتحديات التي يطرحها الفضاء السيبراني، مصدرها العالم الحقيقي، حيث الاشخاص والنشاطات التي تستخدم الانترنت، وترتكز اليه. وقد برز شبه اجماع دولي، حول اعتبار ما هو غير شرعي بمقتضى القوانين في العالم المادي، غير شرعي أيضا في الفضاء السيبراني، وذلك بمقتضى التشريعات الوطنية القائمة. وعليه، فان مبدأ سيادة الدولة، لا بد وان يحترم في هذا الفضاء. غير ان المسألة ليست بهذه البساطة، مع اختلاف القوانين الوطنية على تعريف ما هو شرعي وقانوني، وما هو غير ذلك، اضافة إلى التعقيدات التي ترافق عملية تطبيق مبدأ السيادة الوطنية على المجال السيبراني، نظرا لطبيعته الخاصة.

[1] *A Declaration of the Independence of Cyberspace- BY JOHN PERRY BARLOW - https://www.eff.org/cyberspace-independence*

فقد بدأ هذا المبدأ، يسجل بعض التراجعات أمام حركة العولمة، والانفتاح غير المسبوق، بين الأفراد كما بين الدول، في مختلف مجالات الحياة: من الاقتصاد الدولي إلى التجارة الإقليمية، والتعليم والترفيه، والتجارة الإلكترونية.

٢. أهدافها

تهدف هذه الدراسة، إلى القاء الضوء على عدد من المفاهيم والمسائل، التي ترتبط بالأمن السيبراني، عبر تشريحها، وتشخيص واقعها، ورصد أبعادها. وهي بذلك، تشكل اضافة إلى المحاولات التي سبقت، وتضع بين ايدي الأكاديميين، وكذلك متخذي القرار، مادة تساعدهم على تكوين رؤية واضحة، وبالتالي اتخاذ القرار المناسب. لكنها، بالمقابل، لا تدعي الاحاطة، بكل المسائل، ذات الصلة، ولا تعتبر النتائج المستخلصة قاطعة ونهائية، لاسيما مع التغيرات المتواصلة والسريعة التي تطاول قطاع التقنيات والاتصالات.

وتستند الدراسة، إلى ما تم انجازه حتى اليوم على المستويين الاقليمي والدولي، والى جهود جامعة الدول العربية، في مجال ارساء قواعد الثقة والامان في الفضاء السيبراني، وذلك انسجاما مع دورها في وضع ما جاء من مبادئ، في مقررات القمة العالمية لمجتمع المعلومات، والتي انعقدت في تونس، عام ٢٠٠٥، موضع التنفيذ، حيث شددت جميع الوثائق، على اهمية الأمن والاستقرار والثقة، في الفضاء السيبراني. وتقوم المنهجية المعتمدة، على ركائز: التحديد، والتحليل، والشرح، واقتراح خطوات عملية، تهدف إلى استدراك المخاطر المستقبلية.

هذا وتتوزع المسائل التي سنعالجها، على العناوين الآتية:

- حوكمة الانترنت
- الأمن السيبراني: تعريفات وأبعاد
- المخاطر السيبرانية من الطوارئ الدولية
- الاعتداء السيبراني والجريمة السيبرانية
- الإرهاب السيبراني
- تقنيات المعلومات والاتصالات في المجال العسكري
- مكافحة الجرائم السيبرانية: الاتفاقيات الدولية والاقليمية
- حماية البيانات ذات الطابع الشخصي والحق في الخصوصية
- المرونة السيبرانية في مواجهة المخاطر

الفصل الأول
حوكمة الانترنت

بعيدا عن اي اشتقاق أو غموض لغوي، يدّل مفهوم الحوكمة[2]، على ادراة شؤون المؤسسات، وليس فقط على تولي شؤون الحكومة، كما فهم هذا الامر، من قبل الجهات الحكومية، المشاركة في القمة العالمية لمجتمع المعلومات عام ٢٠٠٣. ولا يمكن الحديث عن حوكمة الانترنت، دون استعراض بعض المحطات في حركة تطور الانترنت، وآليات العمل التي احاطتها، وكونت بيئتها.

١. من مشروع خاص إلى مشروع عام

تعود بداية الانترنت، إلى فكرة إنشاء شبكة معلومات من قبل إدارة الدفاع الأميركية، في عام ١٩٦٩، تهدف إلى وصل الإدارة مع متعهدي القوات المسلحة، وعدد كبير من الجامعات. وأطلق على هذه الشبكة اسم "أربا" ARPA اختصار الكلمة الإنجليزية The Advanced Research Project Administration.

ويقوم مشروع إنشاء الشبكة، على تطوير تقنية تشبيك أجهزة كومبيوتر، تساعد على الصمود في وجه الهجمات العسكرية، وذلك، باعتماد تقنية خاصة، تدعى طريقة إعادة التوجيه الديناميكي Dynamic rerouting. وتستند هذه التقنية، إلى مبدأ تحويل حركة المعلومات والاتصالات، إلى عدد من الوصلات تبعا لتوافرها، في حال انقطاع احدى الوصلات أو تعطلها، ما يضمن عمل الشبكة بشكل مستمر، ودون توقف. لكن الاستخدام الكثيف للشبكة، من قبل الجامعات ومراكز الابحاث، أدى إلى ازدحام حركة العمل عليها، فانشئت شبكة جديدة في العام ١٩٨٣، سميت MILNET، اي الشبكة العسكرية. وخصصت هذه الاخيرة لخدمة المواقع العسكرية، وتم وصلها بواسطة بروتوكول الانترنت مع أربا، التي بقيت في خدمة الجامعات.

فعندما انشئت الإنترنت، شكلٍ أعضاؤها قرية افتراضية صغيرة، حيث الجميع يعرفون بعضهم البعض، لذا فقد صمموا نظاماً مفتوحاً، ما يفسر الاهتمام المحدود، بأمن الأنظمة وحمايتها. وقد بقي الأمن السيبراني حتى وقت قريب، حكراً على مجموعة صغيرة من خبراء الكمبيوتر. لكن فتح الانترنت لمستخدمين جدد، منذ أوائل التَسعينيات، وتنامي عدد المستخدمين بشكل هائل، بلغ أكثر من ثلاث مليارات في أيامنا الحاضرة[3]، أبرز الاستخدامات الواسعة للانترنت، بوجهيها السلبي والايجابي، وجعل الاهتمام بالأمن السيبراني ينتقل إلى سلم الأولويات، في سياسات الدول. فقد تحولت الانترنت، في غضون ما يزيد على الجيل تقريبا، إلى ركيزة أساسية للاقتصاد العالمي والحوكمة، في مختلف أنحاء

[2] *Establishment of policies, and continuous monitoring of their proper implementation, by the members of the governing body of an organization. It includes the mechanisms required to balance the powers of the members (with the associated accountability), and their primary duty of enhancing the prosperity and viability of the organization. - http://www.businessdictionary.com/definition/governance.html#ixzz4C0HiS7T7*
[3] *http://www.internetlivestats.com/internet-users/*

العالم، يتصل بها عدد متزايد في كل يوم من الأفراد، والمؤسسات والأجهزة، الامر الذي استدعى تضافر الجهود لحمايتها.

ويمكن القول، انه منذ البداية، ومن خلال عمل الفريق الهندسي للانترنت IETF-Inernet Engineering Task Force- ، الذي تأسس عام ١٩٨٦؛ والذي عمل بالتعاون والتفاهم مع عدد كبير من الأفراد والمتخصصين، لتطوير الجانب التقني والهندسي من الانترنت، ابتعدت هندسة الانترنت وادارتها، عن اي تدخل حكومي رسمي، أو سلطة، أو مخطط مركزي.

وشكلت الفترة الممتدة بين الاعوام ١٩٩٤ و ١٩٩٨، محطة بدأ معها إدراك الحكومات والهيئات الدولية لاهمية الانترنت، وبدأ التغيير يطاول طريقة العمل غير المركزية التي اعتمدت، لإدارة شؤونها. وهكذا قررت المؤسسة العلمية الوطنية، التي كانت تدير البنية التحتية الأساسية للانترنت، التعاقد مع مؤسسة خاصة، هي Network Solutions Internet، لإدارة أسماء النطاقات. الا ان هذا الامر، اثار تحفظات كثيرة، ونشأ ما يسمى بحرب أسماء النطاقات، والتي انتهت في العام ١٩٩٨، بإنشاء هيئة إدارة ارقام وأسماء الانترنت، ICANN، التي تحولت هي نفسها، إلى محل جدل ونقاش، نظرا لعلاقتها مع وزارة التجارة الأميركية، التي تمارس عليها، نوعا من الرقابة.

ومع القمة العالمية لمجتمع المعلومات، التي انعقدت عام ٢٠٠٣ في جنيف، وعام ٢٠٠٥ في تونس، وضعت حوكمة الانترنت على جدول اعمال الدول، وانتهت قمة جنيف إلى إنشاء فريق عمل خاص بها Working Group on Internet Governance- WGIG-. وفي العام ٢٠٠٦، سجلت ثلاث احداث هامة:

- انتهاء مدة العقد بين وزارة التجارة الأميركية والآيكان.
- انطلاق منتدى حوكمة الانترنت في اثينا، والذي شكل تجربة اولى من نوعها، لاسيما لناحية تعدد الديبلوماسيات multilateral diplomacy، حيث شارك جميع اصحاب المصلحة في مجتمع المعلومات، من القطاعين العام والخاص، ومن مستخدمي الانترنت.
- القمة التي عقدها الاتحاد الدولي للاتصالات في اناتاليا في تركيا، حيث انتخب حمدون توريه، رئيسا للاتحاد، والقى خطابا حول اهمية الأمن السيبراني، والمساعدة على التطوير.

وفي العام ٢٠٠٧، ركزت مناقشات الآيكان على أسماء النطاقات، التي تنشر محتوى اباحيا للراشدين، ما جدد النقاش حول ما اذا كانت مهمة الآيكان تقنية بحتة، ام ان لها علاقة بالسياسات العامة. وناقشت الدول دور الحكومات، وضرورة انخراطها في عمل الآيكان، بحيث تكون مشاركة في القرار.

في العام ٢٠٠٨، لفت استخدام اوباما للانترنت، بشكل مكثف خلال حملته الانتخابية، كما خطابه الداعم للتعددية الثقافية عليها، إلى ما اعتبر في حينه، دعما للتوجه نحو تحويل الآيكان إلى منظمة دولية، والى إقرار مقاربة أكثر انفتاحا لإدارة الانترنت. كما برز مفهوم حيادية الشبكة بشكل قوي، لاسيما في الولايات المتحدة الأميركية. وقد تواجه في هذا المجال، اصحاب محركات البحث، والمواقع الاجتماعية، مع موزعي الخدمات، وشركات الاتصالات، وقطاع الملتيميديا، لان الجهات الثانية،

تفضل اعتماد معايير مختلفة، للخدمات التي تقدمها عبر الانترنت، والتي تقرر على أساسها، التمييز بين المعلومات التي تنتقل.

اما الحدث الاهم، فكان توسع الفايسبوك، وبدء الحديث عن المعلومات الشخصية، وحماية الحق في الخصوصية، والمسائل المتصلة بهما.

وفي العام ٢٠٠٩، تابع اوباما وفريقه، الدفع باتجاه انترنت حيادية، وتم توقيع اتفاق بين الآيكان ووزارة التجارة الأميركية، تخلت فيه هذه الاخيرة، عن دورها المهيمن. وخلال منتدى حوكمة الانترنت في مصر، دعت الصين إلى ادخال المنتدى في نظام الأمم المتحدة، بحيث تعطى الحكومات دورا اكبر، في السيطرة عليها، لكن الولايات المتحدة والبلاد المتقدمة تقنيا، رفضت هذا المقترح.

أما العام ٢٠١٠، فقد تميز بخطاب وزيرة خارجية الولايات المتحدة الأميركية هيلاري كلينتون، عن حرية الانترنت وديمقراطيتها، في مواجهة الحملة التي قادتها الصين، لمنع الوصول إلى المعلومات، وحجب المواقع، واجبارها غوغل على حجب عدد من الخدمات، التي تقدم عادة لاي مستخدم حول العالم. كما تميز أيضا، بحل اشكال استخدام اللغة العربية في أسماء النطاقات، وبالموافقة على اسم النطاق الخاص بالبالغين XXX. كما أعلنت لجنة العلوم والتطوير في الأمم المتحدة، متابعة آلية عمل منتدى حوكمة الانترنت[4]، حتى العام ٢٠١٥.

وفي العام ٢٠١١، توسع نطاق عمل الحوكمة، بحيث أصبح على جدول اعمال معظم الدول، وناقش مسائل البيئة، والطاقة، والأمن، والهجرة. والأهم في ذلك، كان تحول التمثيل في هذا المنتدى، من تقني يتمثل في الخبراء والتقنيين، إلى تمثيل دبلوماسي، على مستويات عليا، وكذلك المتابعة الإعلامية لاعمال المنتدى، من قبل اهم المحطات الاخبارية.

كذلك تأثرت حوكمة الانترنت بالربيع العربي، وتعددت الآراء حول دورها فيه، لكن الشيء الأكيد، ان دورها كان أساسيا، في تطوير الحياة السياسية والديمقراطية للمجتمعات. يضاف إلى ذلك، الاهتمام الذي توليه الوسائل الإعلامية التقليدية بالانترنت، في كل انحاء العالم، لدرجة تخصيص العديد منها فقرات خاصة، بما يحدث عليها، وعلى وسائل التواصل الاجتماعي. وكان هذا العام قد شهد قطع الحكومة المصرية لخدمات الانترنت، على كل الاراضي المصرية، وانعقاد مؤتمرين، الأول في فيينا، حول حقوق الانسان والانترنت، والثاني في هاغ، حول الحرية والانترنت.

وفي الوقت عينه، بدأت الحكومات الممثلة في الآيكان، والتي تحولت سلطاتها مؤخرا إلى الآيانا IANA[5]، وهي السلطة المسؤولة عن اعطاء ارقام عناوين الانترنت، بتقديم اقتراحات حول مبادئ لحوكمة الانترنت.

[4] *The Internet Governance Forum (IGF) serves to bring people together from various stakeholder groups as equals, in discussions on public policy issues relating to the Internet. While there is no negotiated outcome, the IGF informs and inspires those with policy-making power in both the public and private sectors. At their annual meeting delegates discuss, exchange information and share good practices with each other. The IGF facilitates a common understanding of how to maximize Internet opportunities and address risks and challenges that arise.*
[5] *Internet Assigned Numbers Authority*

٢. التفسير الضيق والتفسير الواسع

يرتبط تنظيم الفضاء السيبري، كما وجود القانون فيه، ارتباطا وثيقا ب "حوكمة الانترنت". لا بل أن محتوى القانون ونطاقه، يحددان انطلاقا من المسائل الخاصة بتنظيمها، وباستعمالها، وبالنزاعات الناشئة عنها، وفي إطارها. الا أن موضوع تنظيم الانترنت، يصبح موضوعا شائكا، إلى درجة كبيرة، مع السياسة التي تنتهجها بعض الدول، في مراقبة الانترنت، وفي منع وصول المواطنين، إلى أنواع معينة، من المعلومات، اذ يعتبر هذا، من المواضيع التي تمتنع الدول عن مقاربتها، نظرا لحساسيتها، وللحرج الذي يشكله التطرق اليها. هذا، مع العلم، أن هذه السياسات، تشكل واحدة من المسائل، التي تندرج ضمن "حوكمة الانترنت".

فالنقاش الجدي لموضوع حوكمة الانترنت، يخرج إلى الضوء، مواضيع شديدة الصعوبة، مثل حرية التعبير، والخصوصية، والأمن الوطني، وتطبيق القوانين، والصلاحية على المستوى العالمي، كما موضوع، مبدأ سيادة الدولة. وتعتبر هذه المواضيع، من المسائل الأكثر اثارة للجدل، والاختلاف بين الدول. ولا يخرج مفهوم "حوكمة الانترنت" هو الآخر، عن دائرة الجدل والخلاف.

وقد أبرز تحديد مفهوم "حوكمة الانترنت"، خلافا في وجهات النظر بين الحكومات، والاطراف المعنية الاخرى: كهيئات المجتمع المدني، والقطاع الخاص، عندما تمت مناقشة ما يمكن أن يندرج تحت هذا العنوان. فقد رأى البعض، أنه يتناول إدارة موارد الانترنت، وترتيبات التشغيل، ونقاط التبادل، واقتحام البريد الإلكتروني والتطفل عليه، والأمن السيبراني، والنفاذ إلى المعلومات، والخدمة العالمية، وحقوق الملكية الفكرية، والحق في الخصوصية، وغيرها من الحقوق والحريات الانسانية.

بينما دعا فريق آخر، إلى الاخذ بتعريف أضيق، فيما يتعلق بتدبير وإدارة موارد الانترنت، لاسيما ما يختص منه، بأسماء النطاقات والعناوين.

٣. شراكة لتطوير الانترنت واستعمالها

وكان النقاش حول حوكمة الانترنت، قد أثار ضجة كبيرة، ومزيجا من الخوف وعدم الثقة، ونظريات حول التآمر، واستعراضات قوة، ظهرت بشكل سافر، منذ الأعمال التحضيرية للقمة العالمية لمجتمع المعلومات، في جنيف، ومنذ اللقاءات التي عقدت في إطارها.

الا أن ذلك، لم يمنع التوصل، في حينه، إلى إنشاء فريق عمل خاص بحوكمة الانترنت، في العام ٢٠٠٤. وتألف هذا الفريق، من مجموعة من الخبراء المستقلين، ينتمون إلى أكثر من ثلاثين بلدا، وذلك بقرار من الامين العام للأمم المتحدة. وقد أسندت اليه، مهمة مراجعة الامور، التي يمكن أن تندرج تحت عنوان حوكمة الانترنت، وتقديم النتائج التي يتوصل اليها، نتيجة ذلك، إلى المرحلة الثانية، من القمة العالمية لمجتمع المعلومات.

وبالفعل، فقد قدم هذا الفريق تقريره في العام ٢٠٠٥، موصيا باعتماد التعريف التالي لمفهوم "حوكمة الانترنت"[6]:

«ان حوكمة الانترنت، هي تطوير وتطبيق، من جانب الحكومات والقطاع الخاص والمجتمع المدني، كل بحسب دوره، للمبادئ، والمعايير، والقواعد، والأعراف المشتركة، ولإجراءات اتخاذ القرارات، ووضع البرامج التي تحدد شكل تطور الإنترنت واستعمالها». وقد أشار الفريق، في التقرير نفسه، إلى عدد من المبادئ، التي لا بد من مراعاتها، وهي:

- عدم استحواذ حكومة واحدة، على دور غالب في حوكمة الانترنت، على المستوى العالمي.
- مراعاة التعددية اللغوية، وأصول الشفافية والديمقراطية.
- مشاركة الحكومات، والمنظمات الدولية، والقطاع الخاص، وهيئات المجتمع المدني، في إقرار القواعد، التي تحكم الانترنت.

ويؤشر التعريف المقترح، بشكل واضح، إلى ارتباط "حوكمة الانترنت"، بالمسائل التي تعني الجوانب التقنية. لكن هذا الأمر، لا يبقي المسائل القانونية، أو التشريعية، أو التنظيمية، خارج دائرة تأثيرها.

٤. من الطغيان إلى المساواة

وتعتبر هذه المبادئ، بمثابة رد على الخطر الذي استشعرته، بعض الحكومات والشعوب، نتيجة العلاقة التعاقدية الخاصة، التي تربط حكومة الولايات المتحدة الأميركية بالايكان ICANN، ونتيجة طغيان اللغة الإنكليزية، وعدم القدرة الواضحة للقانون، على التعامل مع تنظيم الانترنت، والنشاط في الفضاء السيبراني، ضمن الاطر المؤسساتية والقواعد التقليدية، التي اعتاد العمل من خلالها. ولعل التعبير الاوضح، عن هذا الاحساس بالخطر، ما نقلته أجواء القمة العالمية لمجتمع المعلومات، التي انعقدت في تونس، من وجهات نظر مختلفة، حول ضرورة اخضاع تنظيم أسماء النطاقات والعناوين على الانترنت، إلى هيئات أخرى، غير الآيكان ICANN، بحيث لا تكون حكومة الولايات المتحدة الأميركية، صاحبة النفوذ الوحيد، في هذا المجال[7].

ويلاحظ في هذا الإطار، اجماع العديد من الهيئات الرسمية والخاصة، على ضرورة انطلاق هذه المبادئ، من مبدأ أساسي، هو المساواة بين الدول والشعوب، في الافادة من امكانات الانترنت، وفي المشاركة في العالم السيبراني، بناء وتنظيما ومراقبة، بحيث لا تتحول تكنولوجيا المعلومات والاتصالات، لاسيما منها الانترنت، إلى مصدر لأنواع جديدة من التمييز والتفرقة بين البلدان والشعوب، أو بين أفراد الدولة الواحدة، ما يخلق بيئة خصبة، للنزاعات والتباعد.

[6] *The report of the Working Group on Internet Governance, published in June 2005, "Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet".*
[7] *U.S. dominance in Internet regulation under fire. Jeffrey Sparshot. The Washington Times. October 10 2005. www.washingtontimes.com" a growing bloc of rich and poor nations wants to strip the U.S. government of its role managing the Internet's most basic infrastructure and hand it to a still-undefined international coalition".*

وفي هذا الاتجاه أيضا، جاء تعليق «مشروع حوكمة الانترنت[8]»، على «بيان المبادئ حول نظام أسماء النطاقات وانظمة العنونة[9]»، الذي صدر عن وزارة التجارة القومية للاتصالات وإدارة المعلومات[10]، منبها إلى خطورة سيطرة الولايات المتحدة الأميركية على قرارات الآيكان، لاسيما وانها، تحمل خطر اثارة ردود فعل لدى الدول التي ترفض ذلك، ما يؤدي إلى تقويض التوافق العالمي حول الانترنت، والاضرار حتى بمصالح المستخدمين والموردين، في الولايات المتحدة [11] الأميركية.

لكل ما تقدم، كان طبيعيا ان يبادر المجتمع الدولي، إلى معالجة التحديات التي تطرح على هذا المستوى، في محاولة للرد على الحاجة إلى تحديد الجهة، التي تملك سلطة القرار في وضع الاسس والمبادئ التشريعية والتنظيمية، من جهة أولى، وتحديد السياسة المفروض اتباعها، لمعالجة المسائل والصعوبات الناتجة عن الانترنت، والتي يمكن مصادفتها في الفضاء السيبراني، من جهة ثانية، وصولا إلى آليات تنفيذ وتطبيق القواعد القانونية والتنظيمية، وفرض الالتزام بها.

ويبقى الأهم ، ذلك الموقف الحازم الذي اتخذته الولايات المتحدة الأميركية، في هذا الشأن، والذي جاء في الرسالة التي وجهتها وزيرة الخارجية، غوندليزا رايس، إلى جاك سترو، وزير الخارجية البريطاني[12]. وقد عبرت رايس، في هذه الرسالة، عن استهجانها للموقف الأوروبي، الذي يدعو إلى إيجاد هيئة جديدة تشرف على إدارة شؤون الانترنت. ورأت فيه، تهديدا لسلامة الانترنت، واعاقة لطبيعة تطورها، الذي يتنافى، ومنطق اخضاعها لاشراف بيروقراطي[13].

واذا كانت الدول المجتمعة في تونس، لم تفلح في أبعاد حوكمة الانترنت، عن دائرة النفوذ الأميركي، الا انها نجحت في اعداد مخطط، لمنتدى عالمي حولها[14]، اجتمع للمرة الأولى في آثينا في العام ٢٠٠٦، وما زال ينعقد سنويا، حتى تاريخنا هذا، لا بل انه بدأ يمتد إلى تكوين فروع اقليمية ومناطقية له، مثل منتدى الحوكمة الافريقي، والمنتدى العربي، إلى جانب منتديات وطنية عديدة.

٥. التقنية والقانون

وتتوزع المسائل التي ترد تحت عنوان حوكمة الانترنت، على محورين اثنين: الأول تقني، والثاني قانوني. الا ان كليهما، يطرحان تحديات على المستوى العالمي، تبدأ بكيفية التنسيق بين الهيئات والحكومات المختلفة، لتصل إلى اعتماد مقاييس ومعايير تقنية موحدة، ونصوص تنظيمية وتشريعية، تستجيب

[8] *Internet Governance Project (IGP).*
[9] *Principles on the Internet's Domain Name and Adressing System.*
[10] *(NTIA) National Telecommunications and Information Administration.*
[11] *The Future US Role in Internet Governance: 7 Points in Response to the US Commerce Department's "Statement of Principles"Concept Paper by the Internet Governance Project www.internetgovernance.org 28 July, 20052- "The US Government's exceptional role as unilateral contracting and oversight authorityfor ICANN, should it continue ad infinitum into the future, will directly contradict the two prongs of the 1998 White Paper policy (internationalization and privatization). Obviously, Internet governance is neither internationalized nor privatized if one national government arrogates to itself the exclusive authority to supervise ICANN, negotiate the terms of its contracts, and approve any changes in the root zone. The policy if unchanged also invites reciprocal actions by other states that may undermine the global compatibility of the Internet and the interests of users and suppliers in the United States".*
[12] *Jack Straw, Secretary of State for Foreign and Commonwealth Affairs*
[13] *Letter from the US secretary of state Condoleezza Rice to the UK foreign minister Jack Straw acting in the role of presidency of the EU., "Burdensome, bureaucratic oversight is out of place in an Internet structure that has worked so well for many around the globe. We regret the recent positions on Internet governance(i.e., the "new cooperation model") offered by the European Union, the Presidency of which is currently held by the United Kingdom, seems to propose just that - a new structure of intergovernmental control over the Internet".*
[14] *International Internet Governance Forum.*

للمسائل القانونية، المستجدة في الفضاء السيبراني. ويشمل ذلك: تحويل أسماء النطاقات إلى عناوين رقمية فريدة[15]، استثمار خدمات الاتصالات، المسؤولية عن الأعمال التجارية والأعمال غير الشرعية على الانترنت، مكافحة الجريمة، التجارة الإلكترونية، استيفاء الضرائب، حماية مستخدمي الانترنت وحماية المستهلك، وغيرها الكثير من القضايا التي يمكن أن تثيرها العلاقات الانسانية على الانترنت، اجتماعية كانت، تجارية، ام اقتصادية.

ويعتبر الجزء التقني، القسم الأول والاهم، في حوكمة الانترنت، كونه الأساس الذي يرتكز اليه قيام العالم السيبراني، وطريقة عمله. اضافة إلى ذلك، يساهم هذا العنصر، إلى حد بعيد، في تقرير ما يمكن اعتماده من أساليب متابعة ومراقبة، ضرورية في التنظيم القانوني، لاسيما على مستوى تقرير قواعد المراقبة، والملاحقة، والتنفيذ، سعيا إلى حماية أمن الانترنت، وصولا إلى حماية الفضاء السيبراني. على ضوء ما تقدم، لا تتماشى المقاربة التقليدية في مقاربة الأمن، المبنية على مسؤولية سلطة واحدة، أو قطاع واحد، مع البيئة الخاصة للشبكة العالمية للمعلومات. اذ لا تملك أية حكومة، أو مرجعية في القطاع الخاص، السلطات الادارية أو القانونية الكافية، على مكونات مجموعات الأنظمة والشبكات المتواصلة، من جهة. ومن جهة أخرى، يستلزم اتساع نطاق مهمة تشغيل الانترنت، وتأمين الموارد الأساسية لها، قدرات مادية، ومؤهلات بشرية، تفوق قدرة اي طرف منفرد، على تأمينها. انطلاقا مما تقدم، كان اللجوء إلى نظام إشراك أكب رعدد من أصحاب المصالح، هو المقاربة الاجدى، والافعل، على مستوى إدارة وحوكمة الانترنت.

٦. مواضيع الحوكمة

يعتبر النظام الخاص بحوكمة الانترنت معقدا، نظرا للمسائل الكثيرة التي يطاولها، والجهات المعنية به، والآليات والاصول والوسائل التي يعتمدها. ويطاول نظام الحوكمة، بحسب المنظور الواسع، اضافة إلى مسائل البنية التحتية، والبروتوكول، وأسماء نطاقات الانترنت، المسائل القانونية، والاقتصادية والتنموية، والاجتماعية الخ...وهذا المنظور، هو الذي اعتمد، بنتيجة التقارير التي قدمت من فريق العمل الخاص بهندسة الانترنت، والقمة العالمية لمجتمع المعلومات، وهو الذي يقرر مواضيع النقاش، التي يتناولها منتدى إدارة الانترنت.

ويمكن تعداد هذه المواضيع على النحو الآتي:

- البنية التحتية، وإدارة الموارد الحرجة للانترنت
- استخدام الانترنت، البريد غير المرغوب فيه، أمن الشبكات، والجريمة السيبرانية
- المسائل القانونية، التي يمكنها ان تؤثر على استخدام الانترنت، والتي تدخل في اهتمامات منظمات قائمة، مثل الملكية الفكرية، والتجارة الدولية.
- الجوانب المرتبطة بالتنمية والتطوير، كبناء القدرات في البلدان النامية

وللمقارنة، نذكر ان منتدى آثينا، نظم لمناقشة مواضيع اربعة: النفاذ، أمن الشبكة، الانفتاح، التعددية،

[15] *Translating domain names into unique numerical addresses read by computers.*

واضيف موضوع خامس في ريو دا جانيرو، عام ٢٠٠٧، هو إدارة الموارد الحرجة للانترنت. ويعتبر منتدىى حوكمة الانترنت، الحدث الأهم الذي تناقش فيه سياسة الانترنت، حيث يجتمع اصحاب المصلحة، الذين يمثلون الحكومات، والقطاع الخاص، والمجتمع المدني. ويعتبر هذا المنتدى المكان الافضل، لمناقشة العديد من القضايا، لاسيما منها، حرية التعبير، وعلاقتها باستخدام الانترنت.

وتورد ديبلو Diplo، وهي منظمة تعنى ببناء القدرات، في مجال حوكمة الانترنت، مواضيع حوكمة الانترنت، تحت عناوين خمسة هي: البنية التحتية والمقاييس، القانون، الاقتصاد، التنمية، الاجتماع والثقافة.

٧. المقاربة القانونية وبناء الثقة

أ- أساس للتنمية

يأتي ثبات العمل واستمراره على الانترنت، في أولويات أهداف الحوكمة، لاسيما على المستوى التقني، نظرا لتأثيره الكبير، على سياسات الانماء، والتطوير، والتشريع. ومن هنا، يفهم الاهتمام بمشاركة جميع الاطراف المعنية، بالبنية التحتية للاتصالات، وباستعمالها، وباستثمارها، سواء في وضع السياسات التنظيمية، أو في وضع القواعد التي تحكم الانترنت.

في المقابل، يعتبر الإطار القانوني والتنظيمي، حاجة ملحة، نظرا لكونه عاملا مؤسسا لعنصر الثقة، ليس فقط في دعم الاستثمار وتقديم نوعية أفضل من الخدمات بكلفة وأسعار تنافسية، وإنما أيضا في إرساء أسس ثقة المواطن في مجتمع المعلومات. وذلك انطلاقا من أن القانون، هو ضمانة الحقوق والحريات[16].

وهكذا تندرج حوكمة الانترنت، في إطار القانون السيبراني، الأمر الذي جعل هذا الأخير، يستحوذ على اهتمام معظم الدول، منذ ما قبل القمة العالمية لمجتمع المعلومات. ذلك ان الانفجار الذي عرفه قطاع تكنولوجيا المعلومات والاتصالات، منذ مطلع التسعينات من القرن الماضي، لم يؤشر فقط إلى الإمكانات الاقتصادية الهائلة التي ترتبط به، بل أيضا إلى الإمكانات والتحولات الاجتماعية والاقتصادية، التي يمكن أن تنتج، عن تمكين المواطنين من هذه التكنولوجيا[17]. اضافة إلى ذلك، تنبهت جميع الدول، إلى ما يمكن أن يعنيه التفرد بحوكمة الانترنت، من قبل احدى الدول، من تفرد في التنظيم والتشريع، لقطاع يعني كل المجتمعات.

ب- أهمية العامل التقني

وتنطلق المقاربة القانونية لحوكمة الانترنت، من الدور التقني الأساسي الذي تلعبه هذه الأخيرة، في

[16] *Communication from the commission to the council, the European Parliament, the European Economic and Social Committee and the committee of the regions- challenges for the European information society beyond 2005. Brussels, 19/11/2004.*

[17] *George Sadowsky, Global Internet Policy Initiative and Internews Network,Raul Zambrano, United Nations Development Programme, Pierre Dandjinou, United Nations Development Programme.Internet Governannce: A Discussion Document prepared for the United Nations ICT Taskk Force. New York, USA / May 24, 2004. 1. Discussions on Internet governance have been taken place for several years and predate the World Summit on the Information Society (WSIS) process. To a large extent, the many globaldebates on the subject grew in volume due to the technology boom of the late 1990s and the heavy involvement and interest of the ICT private sector in the process. The boom not only suggested the apparent emergence of a new economy but also the enormous social and political transformation power that the Internet and related new technologies could deliver into the hands of citizens throughout the globe.*

جمع مختلف شبكات الاتصالات المنتشرة حول العالم. وهذا الدور تحديدا، هو ما يجعلها، باجماع الحكومات والدول والاطراف المعنية المختلفة، التي اجتمعت في تونس، عنصرا أساسيا في البنى التحتية لمجتمع المعلومات، ذا أهمية فائقة للشعوب والحكومات، وذا دور فاعل في مكافحة مشاكل العالم التقليدية: كالفقر، والأمية، والتخلف، اضافة إلى الدور الحيوي الذي يمكنها أن تلعبه، في مجال الأمن القومي والاجتماعي، عبر تسهيلها أعمال السلطة، وتمكينها من ضبط إدارة مسائل حيوية، كالدفاع، والاغاثة، والتنمية، والصحة وغيرها من القطاعات.

ولا تنحصر الإدارة التقنية هذه، عمليا، بجهة واحدة مرتبطة بحكومة معينة، بل اتها تتوزع على عدد من المجموعات والهيئات، المحلية والاقليمية والدولية، التي تعمل ضمن إطار مفتوح من التعاون بينها، والتي تلتزم بمجموعة من المقاييس وأساليب العمل، المتفق عليها عالميا. وتعود هذه المقاييس والأساليب، إلى عدد من المسائل المرتبطة بتطوير البنية التحتية للانترنت، وبهندسة البروتوكولات والاصول المتبعة عليها، وباصول توزيع واعتماد أسماء النطاقات والعناوين، وبأمن المعلومات والأنظمة، وبإدارة الاتصالات، وتنظيم دفق المعلومات[18].

٨. العوامل المحددة لإدارة الانترنت

للإحاطة بالعوامل التي تؤثر في ادارة الانترنت لابد من التطرق إلى السلطات التقنية، الاقتصادية والقانونية.

أ– السلطة التقنية

تحكم طبيعة الانترنت التقنية طبيعة العالم السيبراني، ولهذا نراه يتصف بتقنية عالية، متحركة، وسريعة التحول. و تتحكم هذه التقنية، في تقرير ما يمكن اعتماده من أساليب متابعة، ومراقبة ضرورية، في التنظيم القانوني، للعالم السيبراني، لاسيما على مستوى تقرير قواعد المراقبة، والملاحقة، والتنفيذ[19] .

في المقابل، تتعدد العوامل المؤثرة في إدارة الانترنت. فمنها ما يرتبط بالطبيعة التقنية لشبكة الشبكات، ومنها ما ينتج عن الممارسات السياسية والاقتصادية والقانونية. من هنا، للاجابة على هذا السؤال، لا بد من مراعاة طبيعة الانترنت، والاستخدامات التي تتيحها. فالشبكة العالمية للمعلومات، أو الشبكة العنكبوتية، هي عبارة عن مجموعة من الشبكات المستقلة، التي تتصل ببعضها، عبر استخدام بروتوكول الانترنت، وبروتوكول التحكم في الارسال IP/TCP، للاجهزة العاملة عليها. وفي هذا تجسيد للسلطة التقنية، التي يفرضها الالتزام بمعايير تقنية، وضعت عن طريق التوافق، بين جهات تقنية متخصصة ومعنية بتطوير عمل الشبكة، ما زالت تعمل حتى اليوم، مشكلة بذلك، ما يمكن تسميته، بالسلطة التقنية.

[18] *The Internet Engineering Task Force (IETF),The Internet Architecture Board (IAB), The Internet Society (ISOC) ,which provides the legal umbrella for the activities of the IETF and the IAB, The Internet Corporation for Assigned Names and Numbers (ICANN),The Computer Emergency Response Team (CERT) in the U.S.,The Regional Internet Registries (RIRs),The Internet Assigned Numbers Authority (IANA),The World Wide Web Consortium (W3C),The International Telecommunications Union (ITU),The network operator groups, including RIPE, Apricot, NANOG, APNG, SANOG, AFNOG, SilkNOG,The UNICT Task Force*

[19] القانون والانترنت: تحدي التكيف والضبط- صادر ناشرون- د.منى الأشقر ود. محمود جبور

ويأتي في هذا السياق، الالتزام ببروتوكول معين، للاتصال بالشبكة، أولا، ولاستعمال التطبيقات المرافقة، ثانيا، كالبريد الإلكتروني، والمتصفح، وغرف الدردشة، والمنتديات، والشبكات الاجتماعية، وغيرها. ويعتبر استخدام هذا البروتوكول، قاعدة ملزمة، تنتفي في غيابها، امكانية الاتصال بالشخص، أو بالموقع. ويعتبر بروتوكول الانترنت، مسؤولا عن تحديد كيفية تقسيم المعلومة، إلى رزم يتم نقلها من الجهة المرسلة، إلى الجهة النهائية المحددة لها. وتتم عملية الانتقال هذه، عبر العناوين التي تحملها الأجهزة الموصولة بالانترنت.

ـ الآيكان: صلاحية عالمية وقرارات ملزمة

ظهرت الآيكان في العام ١٩٩٨، مع بداية وضع الانترنت، في تصرف الجمهور الواسع. وقد ترافق هذا الانفتاح مع اعتراضات على احتكار جهة واحدة، لتوسيع أسماء النطاقات العليا، (.org, .com et .net)، ومع ما بدا وكأنه وضع يد الولايات المتحدة الأميركية على الانترنت، من خلال طرحها لإنشاء هيئة خاصة، خاضعة للقانون الكاليفورني، والتي ارتبطت معها بعقد، وقع مع وزارة التجارة الأميركية. وقد سمح إنشاء الآيكان، بمنع احتكار الNetwork Solution Inc.، حيث اسست للسجلات الوطنية لأسماء النطاقات، واعتمدت مبادئ حل النزاعات حول أسماء النطاقات، التي أقرتها المنظمة الدولية لحماية الملكية الفكرية.

فالآيكان هي الجهة المسؤولة، عن ضمان حسن سير عملية انتقال المعلومات، على الانترنت، وتحتفظ لهذه الغاية، بقاعدة بيانات تضم جميع العناوين، مع الجهة المعنية بها، يتم تيويمها بشكل متواصل. وتشكل هذه القاعدة، نقطة محورية، في عمل الانترنت، حيث تقوم ب:

- تخصيص عناوين بروتوكول الانترنت
- اعطاء معرفات البروتوكول
- إدارة أسماء النطاقات العليا
- إدارة أسماء النطاقات الوطنية
- إدارة نظام مخدمات الجذر

وتقوم الآيكان بعملها، في انحاء العالم كافة، عبر مسجلي أسماء النطاقات، الذين تعتمدهم، بناء على التزامهم دفتر شروط، يبين معايير أداء مهام التسجيل، وتعتمد أساليب تسمح بالتعرف على الاشخاص، الطبيعيين والمعنويين، الذين تنطبق عليهم هذه المعايير، وتحدد القواعد والإجراءات، التي تطبق على توفير خدمات المسجلين، من خلال « اتفاقية الاعتماد». وتتمتع الآيكان بصلاحية عالمية، بمعنى ان قراراتها تلزم الاشخاص، والمؤسسات، والحكومات.

ـ أسماء النطاقات

تعتبر أسماء نطاقات الانترنت، كبطاقة الهوية، في تعريفها عن الموقع، وعن الشخص الذي ينشئه.

فلكل جهاز موصول على الانترنت، عنوان يسمى "عنوان بروتوكول الانترنت" IP Address، ويتمثل

هذا العنوان، من الناحية التقنية، بأعداد مفصولة عن بعضها، بنقاط على الشكل التالي: 124.12.56.71. كما يعتبر هذا العنوان فريدا، اذ لا يجوز ان يحمل جهازان عنوانا واحدا. وتتولى إدارة هذه العناوين، وتوزيعها، هيئة متخصصة، هي هيئة الإنترنت للأسماء والأرقام المخصصة (آيكان). كما تتولى هذه الهيئة اعطاء أسماء النطاقات اضافة الى قاعدة المعلومات، التي تحتوي هذه الارقام والعناوين، وتشكل نقطة ارتكاز عمل الانترنت. ولان الآيكان، تملك تقنيا القدرة على فصل بعض الأجهزة، أو الشبكات عن الانترنت، أو حتى ايقاف عملها، يعتبر البعض انها تسيطر عليها، بما يعني، اننا نتحدث هنا، عن القدرة الخاصة بالعنونة.

يبقى لمستخدمي الشبكة، ان يستعملونها بالطريقة التي يريدون، شرط احترام القوانين الوضعية الوطنية، والاجنبية، في حال كانت اعمالهم، تطاول أموالا أو اشخاصا، خارج الحدود. يضاف إلى ذلك، ضرورة احترامهم لبعض القواعد واصول السلوك، الخاصة بها.

لا يوجد تشريع شامل، للتعامل مع المسائل القانونية والنزاعات، التي يمكن ان ترتبط بأسماء نطاقات الانترنت، لدى استعمال اسم مشابه، أو مماثل لاسم تجاري، أو علامة تجارية. لكن العديد من التشريعات الأوروبية، وفي مقدمها التشريع الفرنسي، كما الاجتهاد الوطني والأوروبي[20]، قد تصدى لمعالجة هذه المسائل، استنادا إلى قوانين حماية المستهلك، وحماية العلامات التجارية. وكانت الوايبو– المنظمة الدولية لحماية الملكية الفكرية– ، قد وضعت عددا من القواعد، التزمت بها الآيكان واعتمدتها[21]، في حال نشوب نزاع، وهي:

- حق المدعي في ملاحقة الجهة، التي تستخدم اسما مشابها لماركة أو علامة تجارية، خاصة بمنتجات أو خدمات موجودة سابقا، يملك هو حقوقا عليها، حين يمكن ان يؤدي هذا الاستخدام إلى التباس.
- عندما لا يملك مستخدم الاسم، اي حق، أو مصلحة شرعية، فيما يخص الاسم
- عندما يتم تسجيل الاسم، واستخدامه، عن سوء نية

ويعتبر سوء النية متوافرا في حال:

- لجأ مالك الاسم إلى عرضه للبيع، أو للايجار، أو التخلي عن ملكيته لقاء بدل، على مالك العلامة التجارية، أو المنتج، أو على منافسه.
- محاولة جذب جمهور المستخدمين، بهدف جني الارباح، إلى الموقع، أو إلى اي مكان آخر لمالك اسم النطاق، عبر خلق التباس في ذهن المستخدم، مع الماركة أو الخدمة، التي يقدمها المدعي.
- التسجيل بهدف منع مالك الماركة أو العلامة، من استخدام اسم منتجه، أو خدمته كاسم موقع، لاسيما متى كان هذا التصرف، يندرج في إطار التصرفات العادية، لمسجل اسم النطاق
- تسجيل الاسم، بهدف التشويش على العمليات التجارية للمنافس

[20] *Arrêt de la Cour (troisième chambre) du 11 juillet 2013. / Belgian Electronic Sorting Technology NV contre Bert Peelaers et Visys NV. / Demande de décision préjudicielle: Hof van Cassatie - Belgique. / Directives 84/450/CEE et 2006/114/CE - Publicité trompeuse et publicité comparative - Notion de 'publicité' - Enregistrement et utilisation d'un nom de domaine - Utilisation de balises méta dans les métadonnées d'un site Internet. Affaire C-657/11. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62011CJ0657:FR:NOT*

[21] *http://www.icann.org/en/help/dndr/udrp/policy*

من جهتها، اعتمدت الآيكان، عددا من المبادئ الأساسية، التي تمنع الاستيلاء على أسماء العلامات التجارية، والمنتجات، عبر تسجيلها كأسماء مواقع، وذلك من خلال بنود تعاقدية تفرض:

- تصريحا وتعهدا من صاحب طلب التسجيل، بان طلب التسجيل الذي يقدمه، كامل وصحيح، وبان لا حقوق لاشخاص ثالثين على الاسم الذي يسجله، وبأن هذا التسجيل لا يبتغي تحقيق أهداف غير شرعية، وبان طالب التسجيل لا يقصد استخدام الاسم، خلافا للقواعد القانونية النافذة.
- التزام طالب التسجيل، بالرجوع إلى هيئة التحكيم، الخاصة بحل النزاعات حول اسم النطاق، في حال حصولها، في الاحوال التي أشرنا إليها اعلاه.

وتحمي التشريعات الوطنية الأوروبية، اسم النطاق، كما يعمل الاجتهاد، على ردع الممارسات المخالفة للقوانين، في هذا المجال. وكان القضاء الفرنسي، قد منع استخدام عدد من أسماء العلامات التجارية الفرنسية، من قبل اشخاص، لا علاقة لهم بالمؤسسة[22].

كذلك، يمنع القانون الأميركي منذ العام ١٩٩٩، تسجيل أسماء مواقع، تشكل أسماء علامات تجارية، ومنتجات موجودة، ومشهورة، قبل تاريخ هذا التسجيل[23].

ب– أمان الجذر في ارقام ونطاقات الانترنت

في يوليو ٢٠١٠، قامت كل من ICANN وشركة VeriSign، والإدارة الوطنية الأميركية للاتصالات والمعلومات NTIA، بإضافة مستوى حماية إلى طبعة أسماء النطاقات DNS العليا للإنترنت، من خلال استخدام تقنية تعرف باسم DNSSEC [24]، وهي اختصار امتدادات أمن نظام أسماء النطاقات. وقد تم تطوير هذه التقنية، من أجل حماية مستخدمي الإنترنت، ضد الهجمات التي تؤدي إلى قرصنة أسماء النطاقات، وبعض الأنواع من الإضرار التي يمكن ان تلحق بالخوادم[25]. علمًا بأن استخدام تقنية DNSSEC، يهدف إلى التأكد، من أن المعلومات التي يتم الحصول عليها، من نظام أسماء النطاقات DNS ، لم يتم العبث بها، خلال عملية النقل من مصدر البيانات، إلى الآلة التي تطرح السؤال، بالنيابة عن أي مستخدم.

ويتم هذا الامر، من خلال التوقيع والتوثيق الرقميين، لبيانات DNS. ويعتمد هذا التوثيق، على مفتاح يرتبط بالجذر الخاص بنظام DNS، ومن خلال أي من المفاتيح، أو كلمات المرور أو نظام الأمن. ويخضع هذا المفتاح إلى التحديث، بصفة دورية. وتماشيًا مع أفضل الممارسات، فإن الفريق الذي يعمل في ICANN يتألف من: IANA بصفة مشغل وظائف ، شركاء إدارة ملفات خوادم الجذر الآخرين، كشركة VeriSign المشرفة على صيانة منطقة الجذر، والإدارة الوطنية الأميركية للاتصالات والمعلومات(NTIA).ويعمل هذا الفريق، على "تدوير" أو تغيير الزوج المفتاحي التشفيري، الخاص والعام، أي مفتاح التوقيع الرئيسي، لمنطقة الجذر[26] (KSK)، والجانب العام منه الذي يعمل بصفة المفتاح، لامتدادات DNSSEC الخاصة بالإنترنت.

[22] *Jugement du TGI de paris sanctionne l'enregistrement du nom de domaine la fayette 25 Mai 1999 sur juriscom.net / TGI Nanterre 30 juin 1999 a retenu la contrefacon de titulaire de nom lancome, l'oreal, cacharel etc...*
[23] *la loi Anticybersquatting Consumer Protection act 1999*
[24] *The Domain Name System Security Extensions*
[25] *Servers*
[26] *key signing keys*

ويقصد بتدوير مفتاح التوقيع الرئيسي، KSK، استخراج زوج جديد من المفاتيح، بالإضافة إلى توزيع المكون العام الجديد، على الأطراف التي تقوم على وضع، أو توزيع، أو تشغيل، وحدات حل التوثيق. ويمكن النظر إلى عملية تدوير مفتاح التوقيع الرئيسي KSK، كعملية تغيير أقفال البيت. ففي الحالات التي تكون فيها أسماء النطاقات موقعة منDNSSEC، يتم التحقق من اسم البيانات الموثقة، في كل مرة يحاول فيها مستخدم الإنترنت، الاتصال بخادم محدد باسم نطاق، تتم تجربة المفتاح في القفل، من أجل التحقق من البيانات. وهذا يعني، أن تغيير القفل، دون تحديث المفاتيح، سيؤدي إلى عدم فتح الباب، لان اسم النطاق لن يكون مطابقا، وسوف تفشل محاولة الاتصال.

أما التأثير المحتمل لعملية التدوير، فهو الحاجة ال إجراء توزيع واسع النطاق، وملائم لمرتكز الثقة الخاص بمفتاح التوقيع الرئيسي KSK الجديد.

وعندما استخدم مجتمع الإنترنت، امتدادات DNSSEC للمرة الأولى، حدد شركاء إدارة ملفات خوادم الجذر، بالتشاور مع عدد من اصحاب المصالح، ضرورة إجراء تدوير وتغيير مفتاح التوقيع الرئيسي KSK، عبر مراسمٍ خاصة بالمفتاح، أو بعد مرور خمس سنوات على التشغيل. الا ان هذا الإطار الزمني، بقي مشروطا بالوقائع التشغيلية للإنترنت. ففي العام المنصرم ، ٢٠١٥ ، مثلا، تركز الاهتمام في الآيكان على عملية نقل دور الإشراف إلى IANA[27]، باعتبارها المسألة الأكثر اتصالا بالجمهور، من منظور الاتصالات، لكن ذلك لم يعن توقف العمل، على تدوير مفتاح التوقيع الرئيسي KSK، الذي استمر بشكل مواز. وقد بدأت في أكتوبر ٢٠١٦، عملية الاستعداد الرئيسية الجديدة، لتدوير مفتاح التوقيع الرئيسي KSK، ومن المتوقع ان يتم اكمالها، في مارس ٢٠١٨، علما ان هذا الإطار الزمني، يبقى هو الآخر، عرضة للتغيير، إذا ما استدعت الظروف ذلك. فتدوير KSK، يشبه تغيير كلمة المرور بشكل دوري، لكن تغييره، يتطلب جهودا خاصة.

ج- السلطة الاقتصادية

تلعب القوة الاقتصادية، دورا لا بأس به، في الفضاء السيبراني، عبر التأثير المتبادل، بين القوة الاقتصادية والانترنت. ومن بعض ما يمكن ايراده في هذا المجال، اعتراض بعض الشركات الكبرى[28]، على إدارة الآيكان لأسماء النطاقات، والذي أدى إلى اتفاق[29] بين احدى الشركات المعنية، والآيكان. ويستدل هنا، من الاتفاقيات الخاصة باعتماد التسجيل، والاسعار الخاصة بتسجيل أسماء النطاقات العليا الجديدة، التي سيتم إقرارها، على اهمية الدور الاقتصادي على الانترنت.

وتجدر الإشارة إلى السلطة الاقتصادية، تعني بشكل أساسي الشركات، التي تريد حجز أسماء النطاقات، وتطوير برمجيات، ولكنها تبقى عاجزة، عن ممارسة سلطة معينة على عمل الانترنت على المستوى التقني.

[27] *Internet Assigned Numbers Authority*
[28] *Site Finder and Internet Governance - Jonathan Weinberg. "The lesson of Site Finder, in short, is that the existing domain-name architecture and standards process aresubject to substantial pressure from an aggressively for-profit VeriSign". http://faculty.law.wayne.edu/Weinberg/UOLTJ_1.1.doc%2015(Weinberg).pdf*
[29] *ICANN Board Approves VeriSign Settlement Agreements. http://www.icann.org/en/news/announcements/announcement-28feb06-en.htm*

د- السلطة التشريعية الوطنية

انطلاقا من مبدأ سيادة كل دولة على أراضيها، ومن المبدأ القانوني، الذي يتحمل بموجبه كل شخص، نتيجة أعماله التي تلحق ضررا بالآخرين، يخضع كل مستخدم للانترنت، للقوانين الوضعية الوطنية، ما يؤثر محليا، على عمل الانترنت. وبالتالي، فان القيام بعمل مخالف للقانون الوطني، يؤدي إلى ملاحقة المخالف، أمام المحاكم الوطنية، بحسب القانون الوطني. وبغض النظر، عن تجريم هذا العمل، أو عدم تجريمه، في بلد آخر. فالطبيعة العالمية للانترنت، التي تثير صعوبات في وجه تطبيق القانون الوطني، خارج إطار السيادة، وعلى مواطنين أجانب، لا تحول العمل المخالف للقانون الوطني شرعيا، بسبب عدم تجريمه في قوانين أجنبية، بل ان العكس، يمكن ان يؤدي إلى ملاحقة الفاعل، من قبل سلطات أجنبية.

واذا كانت القوانين الوضعية، لا تلحظ نصوصا، تجرم بعض الافعال على الانترنت، يبقى الانتباه ضروريا، إلى ان الانترنت، لا تعتبر نطاقا خارج القانون، وبالتالي، لا شيء يمنع تطبيق القوانين التقليدية، في حال غياب التشريع الخاص، على العديد من الاوضاع القانونية، الناشئة عن استخدام الانترنت.

ولعل المثال الذي يمكن سوقه هنا، على تأثير القوانين الوضعية على الانترنت، هو إقرار الحق في تسجيل البرامج المعلوماتية، بحسب القوانين الأميركية، وعدم جوازه في القوانين الأوروبية. ففي فرنسا خاصة، وأوروبا عامة، يمنع تسجيل البرامج المعلوماتية والتطبيقات، والبرامج الحرة المصادر، كما يمنع تسجيل المعادلة الحسابية، بينما يسمح بذلك في الولايات المتحدة واليابان. وكان هذا الوضع، قد استلزم مشاورات على المستوى الأوروبي، في محاولة لمواجهة الارتباك، الذي كان يسود السوق الداخلي، بسبب اختلاف التطبيقات الاجتهادية، لمبدأ المنع، لاسيما وان بعض المحاكم، اتجهت إلى إقرار الحق في التسجيل، رغبة منها في الحفاظ على المستثمرين الأوروبيين. فقد أشرت الممارسات في الاتحاد الأوروبي، إلى معاكسة قرار البرلمان الأوروبي، بمنع التسجيل.

يبقى ان هذا التبسيط الذي اعتمدناه، في حديثنا عن السلطات على الانترنت، لا يعطي فكرة وافية عمن يدير الانترنت، لاسيما وان هذه السلطات تتداخل فيما بينها، وتتفرع منها سلطات وهيئات كثيرة، تجعل الحوكمة عملية معقدة. ونشير على سبيل المثال، إلى خضوع عملية تحديد المقاييس والمعايير، الخاصة بالبنية التحتية للانترنت، لصلاحيات هيئات ومنظمات دولية، مثل الاتحاد الدولي للاتصالات، ومعهد مهندسي الكهرباء والإلكترونيات Institute of Electrical and Electronics Enginee، والذي يعنى بوضع معاير خاصة بالشبكات المحلية. يضاف إلى ذلك، التأثير السياسي الذي يبدو جليا، من خلال ممارسات الولايات المتحدة الأميركية، سواء فيما يتعلق بإدارة موارد الانترنت، أو عبر مطالبتها بإقرار الحقوق والديمقراطية عليها.

الفصل الثاني
الأمن السيبراني: تعريفات وأبعاد

١ . تعريفات

يمكن تعريف الأمن السيبراني، بانه أمن الشبكات، والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالانترنت. وعليه فهو المجال الذي يتعلق بإجراءات، ومقاييس، ومعايير الحماية، المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، أو للحد من آثارها في أقسى وأسوأ الاحوال.

ويرتبط هذا الأمن، ارتباطا وثيقا، بأمن المعلومات. فالوصول إلى هذه الأخيرة، أو بثها، أو الاطلاع عليها والمتاجرة بها، أو تشويهها واستغلالها، هو ما يقف، غالب الاحيان، وراء عمليات الاعتداء على الشبكات، وعلى الانترنت.

فالاعتماد على المعلومة، حقيقة لا لبس فيها، تفرض اعتمادا أكثر، على الأنظمة الإلكترونية التي تعالجها.

والحديث عن الأمن، يستدعي تعريف الخطر، أي التهديد الذي يتعرض له النظام[30]، إضافة إلى نقاط الضعف، أو الثغرات التي تعتريه، ومن ثم الإجراءات المفروض اتخاذها، لدفع الخطر. فالتهديد هو نوع الأعمال العدائية، التي يمكن ان تمارس ضد النظام، بينما نقاط الضعف هي مستوى الانكشاف على هذا التهديد، في سياق معين. والإجراءات التي يفترض اتخاذها، لا يمكن ان تقتصر في أي حال من الاحوال على التقنية، بل انها تتناول بناء القدرات، والتوعية، والتدريب، ونقل الخبرات، عدا عن مجموعة من القواعد المحددة والواضحة، التي يفترض اتباعها.

فالخطر يتناول أمن الشبكات وأمن الانترنت، لناحيتين: الأولى، هي البنية التحتية، وما عليها من نقاط دخول وخروج وتخزين، واعتراض للمعلومات. والثانية، عمليات التخريب، والتدمير والتعطيل، التي تطاولها، وتطاول الأموال والاشخاص من خلالها.

ولان للشبكة العالمية للمعلومات، مواصفات تقنية وفنية خاصة، تؤسس لمخاطر معينة، فان اتصال الشبكات بها، يعرض هذه الاخيرة للمخاطر عينها. وبذلك، يمكن تصور تعرض النظام لاعتداء، يجعله يتوقف عن تأدية الخدمات التي كان يقدمها، أو يجعله يعرض أسرار المؤسسات والأفراد، سواء منها الشخصية أو الصناعية والمهنية، أو بما يؤدي إلى تلف البيانات الحساسة، أو بث معلومات مغلوطة.

وهنا، لا بد ان نشير، إلى ضرورة التمييز، بين المعلومات وبين التكنولوجيا وادواتها. فالمعلومة هي ما ينتج عن معالجة البيانات والمعطيات بشكل معين، تستخدم فيه التكنولوجيا، سواء للتجميع، أو للوصول، أو للتخزين، والمعالجة.

[30] يمكن تحدي حمايته

لذا، فان أولى خطوات تحقيق الأمن، هي مراقبة هذه التكنولوجيا، لاسيما في شقها الذي يمثل الاتصالات، ومراقبة حركة انتقال المعلومات، بما يضمن ازالة العوائق امام الوصول إليها، وانسيابها، ويمنع التنصت، سواء من جانب الطرف المنافس، أو من قبل الطرف الذي يسعى إلى الاعتداء. من هنا ضرورة سعي المؤسسات، كما الأفراد، إلى تحقيق أمن الاتصالات، عبر الحفاظ على سريتها، مع ما يمكن ان يطرحه هذا الامر من إشكاليات، تتعلق بمكافحة الجرائم، والحفاظ على الأمن. وبهذا المعنى، يكون الأمن، هو عدم السماح باستخدام النظام، إلا فيما هو معد لأجله، وفي الإطار المسموح به.

فالأمن السيبراني، بحسب التعريف المعطى له، في التقرير الصادر عن الاتحاد الدولي للاتصالات، حول «اتجاهات الاصلاح في الاتصالات للعام ٢٠١٠-٢٠١١»، هو مجموعة من المهمات، مثل تجميع وسائل، وسياسات، وإجراءات امنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية، وموجودات المؤسسات والمستخدمين[31].

وتهدف الحماية، إلى جعل المعتدين يحجمون عن خطتهم، أو إلى منعهم من تحقيقها، والى ضمان حد مقبول من الأخطار، وذلك عبر وضع خطة أمن، تتلاءم والمحيط التقني، البشري، التنظيمي، والقانوني.

الا ان الأمن بصورة شاملة، وأكيدة، ومضمونة، بعيد المنال. فلكل نظام نقاط ضعف وثغرات خاصة به، جعلت البعض يعتبرون قوة اي نظام، انما تقاس بقوة أضعف نقطة فيه. ومما لا شك فيه، ان اهتمامات الأمن، تختلف باختلاف المواد والموارد المعرضة للتهديد. فالمواقع التجارية الخاصة، غير المواقع الحكومية، وهذه الاخيرة، تختلف عن المواقع المالية، والعقارية، كما تختلف عن مواقع التسلية والمقامرة.

تأسيسا على ذلك، يمكن تعريف الأمن السيبراني، انطلاقا من أهدافه، بانه النشاط الذي يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن امكانات الحد من الخسائر والاضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح اعادة الوضع إلى ما كان عليه، بأسرع وقت ممكن، بحيث لا تتوقف عجلة الانتاج، وبحيث، لا تتحول الاضرار، إلى خسائر دائمة.

في مدلوله العام، يعطى الأمن تعريفات عديدة، تنطلق من الإمكانات العسكرية، مرورا بالحفاظ على استقرار النظام، وصولا إلى حماية القيم الجوهرية لمجتمع ما. لكن، وبغض النظر عن تقارب أو اختلاف النظرات الفلسفية والسياسية حول الموضوع، فان الراسخ، هو الخشية التي تبديها معظم الدول حاليا، من تعرض امنها القومي، نتيجة الاعتداءات السيبرانية، لاسيما وان تقنيات المعلومات والاتصالات، قد رفعت منسوب الخطر، عبر اتاحتها مصادر جديدة، متشعبة ومتعددة، وامكانات هائلة، لتحقيقه، مقابل انخفاض نسبة المخاطر وامكانات الانكشاف، في جانب الجهة المعتدية. والدليل على ذلك، هو التنسيق المتزايد بين ادارات الأمن والاقتصاد[32]، اضافة إلى الترابط الذي يراه قادة العالم، بين أمن الفضاء السيبراني، والاقتصاد والأمن القومي.

---

[31] *Trends in Telecommunication Reform 2010-11- ITU-“ The term “cyber security” refers to various activities such as the collection of tools, policies,security safeguards, guidelines, risk management approaches, training, best practices, andtechnologies that can be used to protect the cyber environment and the assets of organizations and Users”.*

[32] *L’institution militaire en France loge, le poste de Haut représentant charge de l’intelligence économique (HRIE), responsable de la coordination des réponses gouvernementales en ce domaine, a savoir le secrétariat général de la défense nationale (SGDN).*

ويلامس الأمن السيبراني الأمن القومي، بشكل جد وثيق. فالتقنيات التي وسعت الآفاق، وأثرت الثقافة، وسمحت للثقافة المحلية بالامتداد إلى المجال العالمي، باتت تهدد الهوية الوطنية والقومية، مع تأثر الاجيال الصاعدة بما يصلها وبما تصل اليه عبر الإنترنت، حيث تبدو الهوية وكانها خاضعة لعملية اعادة تشكيل، من خلال تكنولوجيا المعلومات، وحرص الغالبية العظمى من الناس، على استخدامها في تكوين مجتمعهم الخاص، وبيئتهم المميزة.

فالفضاء السيبراني، كأي مجال آخر، مكان يستحضر الناس فيه قيمهم ومصالحهم، واهتماماتهم المختلفة، التي يمكن ان تتأثر وتؤثر. وبتنا نلاحظ، على سبيل المثال، ان بعض مجموعات المصالح الخاصة، تهدد بالحلول كبديل لهوية يندمج تحت مظلتها، مجموعات أكبر من الناس.

وكان مايكل ماكونال، المسؤول السابق عن الأمن الوطني الأميركي، قد اعتبر، ان الانترنت قد رفعت مستوى الأخطار التي يتعرض لها النظام، بشكل غير مسبوق[33]. وذلك، في إشارة واضحة، إلى التهديدات الجديدة، التي تستهدف الأمن القومي، والتي يمكن ان تتخذ اشكالا غير متوقعة، وتطاول مجالات أساسية وحيوية. كذلك، أعلن الرئيسي الأميركي الحالي، باراك اوباما، ان أمن الفضاء السيبراني، يأتي في مقدمة اهتماماته، معتبرا التهديد الآتي من الفضاء السيبراني، من أخطر المسائل، التي تطرح على المستوى الاقتصادي، كما على مستوى الأمن القومي. وقد ترجم هذا عمليا، بتعيين مسؤول عن أمن الفضاء السيبراني، يكون على اتصال وتنسيق دائمين معه، ويكون عضوا في الأمن القومي، وفي المجلس الاقتصادي الوطني[34].

في هذا الإطار، حددت التوصية الأوروبية الصادرة في العام ٢٠٠٢[35]، الأمن القومي، بانه: «أمن الدولة، والدفاع، والسلامة العامة، ...». وعليه، فالأمن القومي هو جميع الإجراءات القانونية، والادارية، والعسكرية والأمنية، التي تهدف إلى حماية بلد معين، ضد اي نوع من التهديدات والأخطار، التي يمكن ان تعرض سلامة مواطنيه أو اراضيه، أو سيادته، بما فيها سلامة بنيته الحساسة، وبنية الاتصالات والمعلومات.

اما على المستوى العربي، وبالرغم من غياب تعريف واضح للأمن القومي، الا ان هنالك محاولة، قامت بها الامانة العامة لجامعة الدول العربية، باعدادها دراسة في العام ١٩٩٢، جاء فيها: ان الأمن القومي، هو قدرة الامة على الدفاع عن أمنها، وحقوقها، وصيانة استقلالها، وسيادتها على اراضيها، وتنمية القدرات والإمكانات العربية، في مختلف المجالات السياسية، والاقتصادية، والثقافية والاجتماعية، مستندة إلى القدرة العسكرية والدبلوماسية، آخذة في الاعتبار الاحتياجات الأمنية الوطنية لكل دولة، والإمكانات المتاحة، والمتغيرات الداخلية والاقليمية والدولية، والتي تؤثر على الأمن القومي العربي.

وهكذا، يبدو واضحا، انه مع تحول الأنظمة، وتغير انماط الحروب، وموازين القوى، وتطور مفهوم دور الدولة، اتسع مفهوم الأمن القومي، ليشمل السلامة المادية للمواطنين والوطن، والأمن الاقتصادي، والاجتماعي، والانساني.

[33] *McConnell said the Internet has «introduced a level of vulnerability that is unprecedented."Cybersecuritystarts at home and in the office.http://www.google.com:80/hostednews/ap/article/ALeqM5gkZ5sKNT86kqT9TWeDlogVPoASyQD9B469980*
[34] *Loppsi en France et Cyber-securite aux USA http://www.natchers.com/actualite-2009/8239/loppsi-en-france-et-cyber-securite-aux-usa*
[35] *La directive européenne 2002/58/CE, remplacée par la directive 2006/24/CE. La sécurité nationale est "... la sûreté de l'état, la défense, et la sécurité publique..."*

٢. أبعاد الأمن السيبراني

يطاول الأمن السيبراني جميع المسائل الاقتصادية، والاجتماعية والسياسية، والانسانية، وذلك انطلاقا من التعريف المعطى له، على انه قدرة الدولة على حماية مصالحها وشعبها، في مختلف مجالات حياته اليومية، ومسيرته نحو التقدم، بامان، من جهة اولى، ومن كونه يرتبط ارتباطا وثيقا بسلامة مصادر الثروة في العصر الحالي، ونعني بها، البيانات، والمعلومات، والقدرة على الاتصال والتواصل، وهي المحور الذي يتكون حوله الانتاج، والابداع، والقدرة على المنافسة، من جهة ثانية.

لذا، لا بد من التوقف عند أبعاد الأمن السيبراني، على ان نستعرضها كما يلي:

أ- الأبعاد العسكرية

تتراكم الامثلة التي يمكن سوقها، في هذا المجال، لتوضيح الأبعاد العسكرية للأمن السيبراني، وخطورة الهجمات السيبرانية، حيث يمكن ايراد ما حصل في جورجيا، واستونيا، وكوريا الجنوبية، وإيران، كمثال على بعض الهجمات والاختراقات، التي ترجمت ماديا، سواء باندلاع صراع مسلح لاحق، كذلك الذي وقع بين روسيا وجورجيا، أو بانقطاع الاتصال بالانترنت في استونيا، بين الدولة والمواطنين، والتشويش على الادارات الحكومية.

كذلك، ترد هنا، اختراقات أنظمة المنشآت النووية، في إيران، وتحقق امكانات التلاعب بها، مع ما يعنيه ذلك من تهديد للأمن القومي، للدولة المعنية، ومن تعريض السلام الدولي للاهتزاز. في هذا المجال أيضا، يمكن ايراد الاختراق الذي حصل في البرازيل، والمملكة المتحدة، للبنية التحتية للطاقة، حيث انقطع التيار الكهربائي، ما طال بآثاره السلبية ملايين الاشخاص، والمؤسسات والمصالح.

في هذا السياق، وجه خبراء أميركيون، خطابا مفتوحا إلى الرئيس الأميركي، جورج بوش"[36] ، في ايلول ٢٠٠٧، محذرين اياه، من خطر الهجمات السيبرانية على البنية التحتية الأميركية، التي تضم إلى الدفاع، امدادات الطاقة الكهربائية، والمياه، والاتصالات السلكية واللاسلكية، والخدمات الصحية، والنقل، والانترنت.

فالى جانب سيناريو هجمة سيبرانية على مثال بيرل هاربور، يبقى السيناريو الذي تخيله حمدون توريه، حول النتائج الكارثية[37]، التي يمكن ان تتجسد فيها التهديدات، هي افضل ما يمكن ان يعبر عن جدية الامر، وحاجتنا إلى العمل معا، لتحقيق هذا الأمن، لاسيما وان كلفة التقاعس، وانتظار وقوع الكارثة، يجعلان نتائجها أكثر دراماتيكية.

[36] *In an open letter to the US president in September 2007, American professionals in cyber defense warned that «the critical infrastructure of the United States, including electrical power, finance, telecommunications, health care, transportation, water, defense, and the internet, is highly vulnerable to cyber attack. Fast and resolute mitigating action is needed to avoid national disaster.» In the murky world of the internet, attackers are difficult to identify. http://belfercenter.ksg.harvard.edu/publication/18727/cyber_insecurity.html*

[37] البحث عن السلام السيبراني 2011 ...» وهذه الهجمات يمكن أن تأتي دون مقدمات فالحواسيب والهواتف الخلوية تتوقف عن العمل فجأة كما أن شاشات آلات صرف النقد والآلات المصرفية تنطفئ في وجه العملاء وتتعطل أنظمة مراقبة الحركة الجوية والسكك الحديدية وحركة السيارات وتعم فوضى الطرق السريعة والجسور والممرات المائية وتتوقف السلع غير المعمرة بعيداً عن السكان الجائعين. ومع اختفاء الكهرباء تهوي المستشفيات والمساكن والمراكز التجارية بل ومجتمعات بأكملها في غياهب الظلام. ولن تستطيع السلطات الحكومية معرفة مدى الضرر أو الاتصالات ببقية العالم لإبلاغه بالكارثة أو حماية مواطنيها الضعفاء من الهجمات التالية. وهذه هي المحنة القاسية التي يواجهها مجتمع تعرض للشلل بسبب ضياع شبكاته الرقمية في لحظة واحدة. وهذا هو التدمير الذي يُمكن أن ينجم عن نوع جديد من الحروب هي «الحرب السيبرانية».

ب- الأبعاد الاجتماعية

تسمح طبيعة الانترنت المفتوحة، عبر المدونات والشبكات الاجتماعية بشكل خاص، لكل مواطن، بان يعبر عن تطلعاته السياسية، وطموحاته الاجتماعية، بأشكالها كافة. كذلك، تشكل مشاركة جميع شرائح المجتمع ومكوناته، وسيلة لاغناء هذا المجتمع، وتطويره، بما تتيحه من فرص للاطلاع على الافكار، والمعلومات، المختلفة، وبما تكونه من حاجة لدى الجميع، في الحفاظ على استقرار الفضاء السيبراني، والمجتمع الذي يرتكز اليه. والمعلوم، ان انفتاح مجتمع ما، على مجتمع آخر، يؤسس لتبادل خبرات، وافكار، وتكوّن حاجات جديدة، وآفاق تعاون وتكامل.

يضاف إلى ذلك، ما تقدمه الانترنت، من امكانات وقدرات، للمجالات العلمية، والثقافية، والخدماتية، حيث تسمح بالوصول إلى مناطق بعيدة، والى فئات محددة، ككبار السن، والمرضى، وغيرهم من ذوي الاحتياجات الخاصة. هذا عدا عن الدور الذي يمكن ان تؤديه، في تبادل المعلومات، في اوقات الازمات الانسانية والكوارث، بحيث تتأمن المساعدات، وتوزع بالسرعة المطلوبة. ولا تقف الأبعاد الاجتماعية، عند حدود توفير اطمئنان المواطن إلى حياته اليومية، والافادة من طاقات تقنيات المعلومات والاتصالات، في تطوير نشاطاته المختلفة، بل تتعداها، إلى صيانة القيم الجوهرية في المجتمع: كالانتماء، والمعتقدات، اضافة إلى العادات والتقاليد، عبر إنشاء المجموعات، التي تهتم بنشر الوعي حول هذه المسائل.

في هذا السياق، يأتي التشديد من قبل المنظمات والهيئات الدولية، على نشر ثقافة الأمن في الفضاء السيبراني، وضرورة تعاون المجتمع، بكل مكوناته، على تحقيقه وضمانه. فمما لا شك فيه، ان المخاطر السيبرانية، تطاول المجتمع ككل، سواء، بسبب ارتكاز الخدمات الحيوية، كالطاقة، والنقل، والصحة، والاتصالات، وغيرها، على ما تقدمه تقنيات الاتصالات والمعلومات، من امكانات، أو عبر ما يضخ من محتوى في الفضاء السيبراني. فالمحتويات غير المشروعة، وغير المرغوب بها، ذات تأثير سلبي أكيد، على اخلاقيات مجتمع معين، وعلى ارتفاع نسبة الممارسات الجرمية. أما الأمثلة التي تساق هنا فكثيرة، ونذكر منها: الاباحية، والترويج للاتجار بالممنوعات، والدعارة، والإرهاب، والتجنيد لقضايا تمس الأمن والسلام الدوليين. وعليه، لا بد من بناء مجتمع مسؤول، ومدرك لمخاطر الفضاء السيبيراني، قادر على التعامل بحد أدنى من قواعد السلامة، مع إدراك للعواقب القانونية، التي يمكن ان تترتب على بعض التصرفات، التي تمارس في الفضاء السيبراني.

ج- الأبعاد السياسية

تتمثل الأبعاد السياسية للأمن السيبراني، بشكل أساسي، في حق الدولة في حماية نظامها السياسي، وكيانها، ومصالحها الاقتصادية، التي تعني، حقها وواجبها في السعي إلى تحقيق رفاه شعبها، في وقت تؤثر التقنيات، في موازين القوى داخل المجتمع نفسه، حيث أصبح بامكان المواطن، ان يتحول إلى لاعب أساسي، في اللعبة السياسية. كما أصبح بامكانه الاطلاع، على خلفيات ومبررات القرارات السياسية، التي تتخذها حكومته، عبر الكم الهائل من المعلومات، التي يمكنه الوصول اليها، أو النبي يمكن ان توزع وتنشر على الانترنت، وبقية الأجهزة التي توصل بها.

بالمقابل، لا يتوانى العاملون في الشأن السياسي، عن الافادة مما تقدمه هذه التقنيات، للوصول إلى أكبر شريحة ممكنة من المواطنين، والترويج لسياساتهم، في العالم. وغني عن البيان، مدى التأثير الذي يتركه هذا الامر، بغض النظر عن صحة السياسات، والمبادئ والمواقف، التي يروج لها. فقد استخدم اوباما، مثلا، الشبكات الاجتماعية بشكل كثيف، خلال حملته الانتخابية. كما تركت التسريبات، لآلاف الوثائق الدبلوماسية السرية، عبر الويكيليكس، أثرا سلبيا على العلاقات بين الدول، وعلى مصداقيتها.

د- الأبعاد الاقتصادية

يرتبط الأمن السيبيراني، ارتباطا وثيقا بالاقتصاد. فالتلازم واضح، بين اقتصاد المعرفة، وتوسع استخدام تقنيات المعلومات والاتصالات، كما بالقيمة التي تمثلها البيانات والمعلومات المتداولة، والمخزنة، والمستخدمة، على كل المستويات. كذلك، تتيح تقنيات المعلومات والاتصالات، تعزيز التنمية الاقتصادية لبلدان كثيرة، عبر افادتها، من فرص الاستخدام، التي تقدمها الشركات الدولية، والشركات الكبرى، التي تبحث عن إدارة كلفة انتاجها، بافضل الشروط. الا ان هذا الواقع المشرق، يطرح مسائل مختلفة، سواء منها ما يتعلق بحماية مقدم الخدمة، والعمل، أو بحماية المستهلك على الانترنت.

يضاف إلى ذلك، دخول العالم عصر المال الإلكتروني، ضمن بيئة تقنية متحركة، بعد إطلاق خدمات المحفظة الإلكترونية، اذ تتزايد استثمارات المصارف، والمؤسسات المالية، في مجال المال الرقمي. وتتنافس الشركات، على اصدار تطبيقات، تسمح بآليات دفع آمنة، وبحفظ المال في المحفظة الإلكترونية، وبالايفاء من خلالها، وباستخدامها كرصيد افتراضي. وقد وضعت بعض الدول تشريعات خاصة بهذا المال[38]. وغني عن القول، ما يمكن ان يثيره هذا الامر، من صعوبات، وما يتطلبه من تشريعات، للحد من بعض الجرائم الاقتصادية والمالية الخطرة، والعابرة للحدود، كتبييض الأموال، والتهرب من الضريبة.

ويربط المسؤولون عن مقدرات الحكومات، وسياساتها، بين الأمن والنمو الاقتصادي، بشكل واضح[39]. فالأمن السيبراني، يضمن ركون الجمهور، إلى الخدمات التي تقدم بواسطة تقنيات المعلومات والاتصالات، كما يضمن الاقبال عليها، بما يترجم عمليا، بتطوير اسس اقتصاد سليم. ولعل الدليل الاوضح، على هذه القيمة، هو استهداف هذه المعلومات، منذ القديم، سواء من خلال عمليات التجسس الصناعي والعسكري التقليدية، أو من خلال الاعتداء على الملكية الفكرية. هذا عدا عن التأثيرات المالية السلبية، التي يتركها، الاعتداء على انظمة المعلومات، وتعطيلها، كما سرقة نتائج ابحاث، أو غيرها من معلومات، أو كتفشي الفيروسات، على غرار ما حصل، مع فيروس الحب[40]، والذي انطلق من الفيلبين، في العام ٢٠٠٠.

[38] *Electronic money regulations 2011 (EMR 2011) & the payment Services Regulations 2009*
[39] *Senators Unveil Major Cybersecurity Bill Measure Would Update FISMA, Encourage Sharing of Cyber threats By Eric Chabrow, February 14, 2012. "Sen. Susan Collins, R-Maine, one of the bill's sponsors, said in a Senate speech. "The threat is not just to our national security, but also to our economic well-being." http://www.govinfosecurity.com/articles.php?art_id=4506&opg=1*
[40] *« If you're Cisco and you're making $7 million a day online, and you're down for a day, you've lost $7 million. That's where you start. There were estimates that the "Love Bug" virus did damage in the billions and billions of dollars. That scale leaves most people saying, "That's beyond any kind of comprehension." http://www.pbs.org/wgbh/pages/frontline/shows/hackers/risks/cost.html*

هـ- الأبعاد القانونية

يرتب النشاط الفردي والمؤسساتي والحكومي، في الفضاء السيبراني، كما أسلفنا، نتائج قانونية، وموجبات، تستدعي اهتماما، لجهة إيجاد القواعد الخاصة، بحل النزاعات التي يمكن ان تنشأ عنها. لذا، لا بد من مراعاة بعض التحولات، التي رافقت ظهور مجتمع المعلومات. فالى الحقوق الأساسية، والحريات الانسانية المعترف بها، في الدساتير والشرعات الدولية، اضيفت حقوق أخرى، كحق النفاذ إلى الشبكة العالمية للمعلومات[41]، كما توسعت بعض المفاهيم، لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الإلكترونية، والحق في إنشاء التجمعات على الانترنت، كما الحق في حماية ملكية البرامج المعلوماتية.

كذلك، برزت موجبات جديدة، ذات انعكاسات اقتصادية، ومنها، على سبيل المثال: موجب الاحتفاظ ببيانات الاتصالات، وموجب الابلاغ عن مخالفات وجرائم خاصة بالمحتوى، لما يعنيه هذا الامر، من كلفة خاصة بحفظ المحتوى وادارته. ويبقى ان المحور الأساس، في حماية الاشخاص الطبيعيين والمعنويين، على السواء، تبقى ضرورة حماية البيانات، لاسيما الشخصية والحساسة منها، اضافة إلى حماية الحق في الخصوصية.

وذلك يضاف إلى ما يتوقع من تحولات على مستوى سياسات القطاعات الصناعية، والتجارية، على ضوء الحاجة إلى اعادة صياغتها، بما ينسجم مع توسع استخدام الشبكات الاجتماعية، والمسائل القانونية التي لا بد وان تثار، على مستوى حماية المستهلك، والخصوصية، والبيانات الشخصية، وحقوق العمال والمستخدمين، والملكية الفكرية. فالسنوات القادمة، لا بد وان تشهد، تصاعدا في أعداد، الأعمال الجرمية، والممارسات غير القانونية، في الفضاء السيبراني، ما يعني عمليا، ازدياد عدد القضايا التي سترفع امام المحاكم، ما يستدعي، إعداد البيئة التنظيمية والتشريعية، وبناء قدرات هيئات المكافحة والحكم.

ومما لا شك فيه، ان النزاعات القانونية ستطاول: الإعلان الذي يرتكز إلى اطياف مستخدمي الانترنت، انطلاقا من اهتماماتهم البحثية، أو المواقع التي يزورونها، والاختراقات، والتسريبات للبيانات الشخصية، والمالية، سواء منها المقصودة أو غير المقصودة، ومسؤوليات الجهة التي تملكها، أو تديرها، والحق في تصحيح البيانات الشخصية، ومحوها، وتعديلها.

[41] *General Assembly- Human Rights Council Seventeenth session - Agenda item 3 - Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development- Report of the Special Rapporteur on the promotion and protection of the right to freedomof opinion and expression, Frank La Rue. 16 May 2011- A/HRC/17/27-p:16*

الفصل الثالث
المخاطر السيبرانية

١ . مؤشرات مقلقة

مع الاعتماد المتزايد، في حياتنا اليومية، على الأنظمة المعلوماتية، والأجهزة المتصلة بالشبكة العالمية للمعلومات، وتشعب طبيعة هذه الأجهزة، من هواتف خليوية، واجهزة حوسبة شخصية، يزداد عدد المتصلين بالفضاء السيبراني، وتزداد احتمالات الاعتداءات والجريمة. فقد أشار تقرير صادر عن ماكينزي، إلى توقع زيادة المعلومات الرقمية، بمعدل ٤٤٪ ، خلال الاعوام الممتدة من ٢٠٠٩ إلى ٢٠٢٠ [42]. كما يشير العديد من التقارير، إلى توالي حوادث اختراق الأنظمة وسرقة البيانات وتسربها، كاختراق انظمة معلومات سوني، التي نتج عنها تسرب بيانات مليون مستخدم[43]. فالمعلومات التي تضخ، وتنساب، وتحفظ، في الفضاء السيبراني وعبره، من اهم الموجودات التي يسعى اليها، جميع المعنيين بهذا الفضاء، دون استثناء. فالشركات، والحكومات، ومستخدمو الانترنت، يلاحقون المعلومات، كل بحسب أهدافه.

وتصدر الأخطار والتهديدات السيبرانية، عن أعمال قصدية، كالاختراقات والاعتداءات، وأعمال غير قصدية، كالاهمال، وقلة الوعي والادراك.

ويمكن توزيع الأخطار، في الفضاء السيبراني، انطلاقا من أهدافها، بين ما يطاول الدول، وما يطال الاشخاص، وممتلكاتهم وأموالهم. ويندرج في إطار الفئة الأولى، كل ما يعرض الأمن القومي، والعسكري، والاقتصادي، والاجتماعي، ويهدد البيئة التحتية والحرجة للدول، وأسواق المال والقطاعات المصرفية، والسلم الدولي، والمنشآت النووية، والمؤسسات الصحية، وقطاعات النقل بكل أنواعه: البري والبحري والجوي، ورفاه الشعوب. بينما يندرج في الفئة الثانية: سرقة البيانات الشخصية، وتسريبها، واستخدامها دون اذن، ودون وجه حق، وسرقة الأموال، واختراق انظمة المعلومات، والاعتداء على الملكية الفكرية، والصناعية، والعلامات التجارية. كما تشمل هذه الفئة أيضا: الاحتيال، والبريد غير المرغوب فيه، والجرائم ضد الاطفال، والمحتوى غير المشروع، وغيرها الكثير مما يعتبر جرائم سيبرانية، ضد الاشخاص وضد الأموال.

[42] *Mckinsey noted in its july 2011 report*
[43] *In April 2011 sony acknowledged a breach into its PlayStation network*

٢ . المرونة السيبرانية في مواجهة المخاطر

إذا، مع بروز الممارسات الخطرة، والأعمال الجرمية على شبكة الانترنت، كان لا بد للدول من ان تواكب التطور التقني، وان ترفع التحديات الأمنية والاجتماعية التي بات الفضاء السيبراني، يطرحها ويجددها، مع كل صباح.

من هنا، يحتاج التصدي للمخاطر السيبرانية، ولتحديات الأمن السيبراني المعقدة إلى إرادة سياسية، تضطلع بوضع وتنفيذ استراتيجية، لتنمية البنى الأساسية والخدمات الرقمية، قابلة للتنفيذ، وسهلة الإدارة، فاعلة ومتماسكة. يضاف إلى ذلك، ضرورة توفير مستوى كاف من أمن الأنظمة المعلوماتية، ووسائل الاتصالات، يساعد على مواجهة مخاطر التكنولوجيا والمعلومات، لضمان أداء سليم للحكومات والمنظمات، لاسيما مع الاستخدام الشائع والواسع للتقنيات، والاعتماد المتزايد عليها، في إدارة البنى التحتية الحرجة، ما يمكنه تهديد أداء المؤسسات، على نحو خطير، يصل ربما إلى تقويض سيادة الدولة.

أ- تلقي الصدمات والاستمرارية

يهدف الأمن السيبراني، إلى مساعدة الأفراد والدول والمنظمات المختلفة، على حماية أصولها ومواردها، من النواحي التنظيمية، والبشرية، والمالية، والتقنية، والمعلوماتية، بحيث تتمكن من الاستمرار باداء مهماتها. أما الهدف النهائي، فهو ضمان عدم تضررها بشكل دائم، لدى حدوث أي اعتداء أو حادث، عبر تقليل احتمالات تحقق أي تهديد، والحد من الضرر الناجم عنه، وضمان استعادة العمليات العادية لحالتها السابقة، خلال مدة زمنية مقبولة، دون تكلفة عالية. وهذا ما يعرف بالمرونة السيبرانية[44].

وتعتبر هذه الاخيرة، أحد أهم المسائل والتحديات التي لا بد من مواجهتها، في مسيرة بناء الثقة، في الفضاء السيبراني، حيث تتصاعد التهديدات وتبرز التعقيدات بشكل مستمر، نتيجة الاعداد الهائلة من المهمات، التي توكل إلى الأنظمة والأفراد القيمين عليها، وتوسع نقاط الاتصال بين الأنظمة، واعتمادها على بعضها البعض، في إدارة تدفق المعلومات، وحفظها، وتوزيعها، وغيره من عمليات معالجة المعلومات. فأنظمة الاتصال بين الاشياء، كتلك الخاصة بالسيارات ووسائل النقل الاخرى، تتصل بأنظمة الأمن والصحة والطقس وغيرها. وهذا يعني، تضافر الخصائص، والاعدادات المختلفة للبرامج والأنظمة، التي تفرض الانتباه إلى ما هو غير آمن، أو ما هو حساس، بحيث يتم تجنبه، وتأمين الحماية اللازمة له.

يضاف إلى ذلك، ان الحوادث والاختراقات، التي يمكن ان تقع، لا يمكن توقعها خلال عملية هندسة البرامج والأنظمة، بما يجعل السيطرة عليها أو تلافيها، شبه مستحيل أحيانا كثيرة. فيمكن مثلا ان

[44] *Exploring associations between resilience and construction safety performance in safety networks. "Resilience engineering is a paradigm for safety management that focuses on how people cope with complexity under pressure to achieve success (Wybo et al. 2006; Resilience Engineering Network, 2008). Wreathall (2006) associates resilience with the ability of an organization to keep, or recover quickly to, a stable state, allowing it to continue operations during and after a major failure or in the presence of hurdles. Thus, resilience includes both the ability to avoid failures and losses, as well as the ability to respond effectively after these have occurred. "https://www.researchgate.net/publication/283676719_Exploring_associations_between_resilience_and_construction_safety_performance_in_safety_networks*

يستمر النظام بالعمل، في الوقت الذي تتراجع نوعية الخدمة التي يقدمها، أو ان يتوقف نظام التشغيل، أو تتدهور نوعية أدائه. ويمكن ان تقع هذه الحوادث نتيجة أخطاء، أو نقاط ضعف خاصة بالبرنامج، أو كوارث طبيعية، أو استعمال غير سليم من قبل مستخدمي النظام أو البرنامج، أو أيضا نتيجة اعتداء جرمي.

وعليه، لا بد من تحديد المخاطر، ونقاط الضعف، والثغرات، والتهديدات، وتحليلها، وفهمها لوضع الإجراءات الكفيلة بمكافحتها، وبحماية الأنظمة والبرامج.

٣. مصادر المخاطر

في عالم تلتصق فيه النشاطات الانسانية، بكل اشكالها، بأنظمة المعلومات والاتصالات، لا بد لسياسات المرونة، من لحظ مروحة واسعة من مصادر المخاطر، التقنية، والانسانية، والقانونية، التي تعني البنية التحتية العالمية، والخدمات الدولية كالانترنت، اضافة إلى الأجهزة الفردية المتصلة بها.

وعليه، من الضروري، لدى وضع سياسات المرونة والحماية، من ملاحظة عدد من المستويات، التي تتأثر وتؤثر ببعضها البعض، لدى حدوث خلل في اي منها: المستوى العالمي العام، المستوى الوطني، المستوى المؤسساتي، المستوى المعلوماتي (من معلومات)، المستوى التقني، المستوى المادي. وبالتالي، يفترض تحليل المخاطر وتحديد التهديدات الخاصة بكل من هذه المستويات، اضافة إلى التأثيرات الجانبية والمتبادلة لكل منها على الاخرى. ويمكن في هذا السياق الاعتماد على أدلة، تقول بأن التهديد يساوي احتمال وقوعه، اضافة إلى نتائجه وتأثيراتها.

وتتنوع مصادر التهديدات والمخاطر، نسبة إلى مستوياتها. فمن وجهة النظر التقنية مثلا، يمكن ان تصدر عن خطأ، أو عن ثغرة في النظام، أو عن اعدادات وتكوين البرامج والأنظمة. كما يمكن ان تصدر عن سؤ استخدام قصدي، أو غير قصدي، أو عن هجوم أو اختراق داخلي أو خارجي، أو عن عوامل طبيعية. وعليها تضاف إلى معادلة احتساب التهديدات والمخاطر، نقاط الضعف، والعنصر البشري، كي تأتي إجراءات وترتيبات اعادة الحال إلى ما كان عليه، بعد وقوع الحادث، فاعلة ومناسبة.

أما لجهة المصادر الاخرى، فنميز بين الاعتداءات الصادرة عن الأفراد، وتلك الصادرة عن الدول. فبعيدا عن الصراعات العسكرية، وخارج عمليات التجسس، يقوم أفراد أو عصابات، باعتداءات على ادارات حكومية وطنية أو اجنبية. لكن هذه الاعتداءات، لا ترقى إلى خطورة تلك التي تقوم بها الدول، لاختلاف القدرات والإمكانات المتوافرة، كما انها ليست مفتوحة على نفس الأساليب، والوسائل، التي تؤدي إلى المخاطر العسكرية.

وبالرغم من تحول عمليات التجسس، والجرائم السيبرانية الموجهة من قبل دول، إلى ممارسات يومية على الشبكة العالمية للمعلومات، نتيجة فشل التعاون بين البلدان المختلفة، يبقى خطر اندلاع حروب كنتيجة لها قائما، نتيجة حسابات خاطئة لنتائج هذه الأعمال، ومدى تأثيرها. ولا يمكن تجنب ردات الفعل الانتقامية على هذه الأعمال، أو التهديد بها لردع الجهة المعتدية، سواء ضمن إطار الصراع، أو خارجه. فالوسيلة الأنجع لذلك، هي تبيان وتحديد النتائج العملية والمحسوسة، للاعتداءات الموجهة والمقصودة.

وربما يكون الهاكرز البريطاني "تريك" Trick، الذي يقود فريق الهاكرز المعروف ب "تيم بويزن" TeaMpoisoN، المثال الاوضح، على الاعتداءات الفردية، التي يمكن ان تتحول إلى اعتداءات على البلدان، ورجال السياسة، وأمن الدول. فقد انضم هذا المخترق، بعد خروجه من السجن في بريطانيا، إلى تنظيم الدولة الإسلامية، في سوريا، حيث يتولى تدريب عناصره، على الاختراق والتجسس.

وكان هذا الشخص، قد اخترق نظام شركة بلاكبيري، عندما أعلنت أنها ستقوم بمساعدة الشرطة البريطانية، في كشف مشاغبي الاحتجاجات، التي عمت لندن سنة ٢٠١١، كما اخترق الايميل الشخصي لرئيس الوزراء السابق طوني بلير[45]، وسرق معلوماته وصوره ورسائله، وقام بنشرها على الإنترنت.

وكان فريق TeaMpoisoN، قد نشر الأرقام السرية، الخاصة بمسؤولي أحد المواقع التابعة لوكالة الفضاء الأميركية NASA، كما قام في العام ٢٠١٢، بإعداد برنامج، يقوم بالاتصال على الخط الساخن الخاص بمكتب "مكافحة الإرهاب" في بريطانيا، ويرسل اتصالات عشوائية مكررة، أدت إلى تعطيل هذا الخط.

كذلك، قام بخداع ضباط الأمن في جهاز MI6[46]، وهو وكالة الاستخبارات العسكرية السري، عبر اختراق جهاز أحد العناصر، وتسجيل مكالمات داخلية MI6 تم نشرها على الإنترنت، ما أحرج مكتب مكافحة الإرهاب. وكان الفريق نفسه، قد اخترق أحد البنوك الإسرائيلية، خلال الحرب على غزة، ونشر بيانات بطاقات ائتمانية لأكثر من ٢٦ الف اسرائيلي، قام باستخدامها، في طلب " البيتزا".

٤. أنواع من المخاطر

تتنوع الممارسات التي تهدد الأمن السيبراني، بتنوع أهدافها، كما وبتنوع الجهات ، التي تعتمدها، ويمكن ايراد بعضها، على الشكل الآتي:

- التعرض لسرية الاتصالات، التي تطال البريد الإلكتروني، والدردشة، ونقل الملفات، والدخول إلى الأنظمة، للاطلاع على المعلومات دون اذن. ويشابه هذا، التنصت على المخابرات الهاتفية، والاطلاع على البريد الشخصي، ودخول المنازل لتفتيشها، ما يتطلب عادة، وبحسب القواعد القانونية، اذنا مسبقا، من قبل السلطات المختصة، في البلاد التي تقوم على احترام القاعدة القانونية. وتعتبر هذه الأعمال، في غير تلك الحالة، سواء قام بها الأفراد، أو قامت بها السلطات العامة، جرائم اعتداء، على الحريات والحقوق الشخصية.
- التلاعب بالمعلومات الموجودة في نظام معين، وتشويهها أو اتلافها، سواء عبر الاقتحام اليدوي، أو عبر ارسال برامج وفيروسات متخصصة بذلك. ففي هذا اعتداء على الملكية، وعلى حقوق التمتع والتصرف بها. يضاف إلى ذلك، التعرض لسلامة عمل المواقع، الشخصية منها والتجارية، عندما تتوفر نية الاضرار، بغض النظر عن تحقق الضرر المرجو، أم لا.
- الجرائم العادية التي تستخدم الانترنت في تنفيذها، كالسرقة والغش والخداع، والتغرير بالقاصرين، وتسهيل الدعارة، والترويج لنشاطات مخالفة للقانون، والاعتداء على الملكية الفكرية. فكل هذه

[45] *Team Poison› hacker who posted Tony Blair›s details is jailed - http://www.telegraph.co.uk/technology/internet-security/9432459/Team-Poison-hacker-who-posted-Tony-Blairs-details-is-jailed.html*
[46] *Military Intelligence, Section 6*

جرائم تعاقب عليها القوانين الوضعية، ونميل إلى القول هنا، انها لا تتطلب بالضرورة إقرار نصوص جديدة، بل تعديل ما هو موجود، ليتناسب مع العناصر المادية الجديدة، التي يدخلها الفضاء السيبيري، من خلال طبيعته الخاصة. ففي احدى القضايا التي عرضت على المحاكم الأميركية، استخدم أحد الاشخاص البريد الإلكتروني، ليراسل احدى الجمعيات طالبا للمساعدات، مقدما نفسه على أنه سيدة، تعيش في مخيم للاجئين في نيجيريا[47]. ومن الاطلاع على وقائع القضية، نلاحظ عدم وجود ما يميزها عن عمليات الغش، التي تتضمن انتحالا للشخصية، سوى لجوء هذا الشخص، إلى استعمال تكنولوجيا المعلومات والاتصالات، في ارتكاب جريمته.

- الجرائم التي تندرج في إطار الجريمة المنظمة، والتي تهدد أمن الأفراد والدول، على السواء، في الفضاء السيبيري، وفي الفضاء التقليدي. وتأتي في هذا الإطار، جرائم تبييض الأموال والإرهاب، والتي سنعرضها بالتفصيل في فصل لاحق.

٥. المسؤولية في الحوكمة والسيادة

من هنا، لا بد للدول، من مقاربة مسألة ردع التهديدات التي يمكنها ان تؤدي إلى الاخلال بالأمن الدولي، استنادا إلى عدد من الحقائق، ومنها: اصرار بعض منها، على التنافس غير الشريف، الإمكانات العالية لاندلاع حرب، نتيجة لخطأ في احتساب نتائج التصرفات العدوانية والجرمية. ولأن المجال السيبراني، ليس مجالا مختلفا عن غيره، فان الدول ستمارس فيه ما تمارسه عادة في المجالات الاخرى، وبالتالي فمن غير المنطقي الحديث عن غياب التهديد، ما دام من غير الممكن نزع السلاح فيه.

ويبقى على الدول، التسليم بضرورة العمل على الحد من مخاطر نشوب صراعات عسكرية، عبر اخضاع الاعتداءات والتجسس، لقواعد القانون الدولي الحالي، والعمل على إيجاد اتفاق دولي، تلتزم فيه الدول الأعضاء في الأمم المتحدة، عدم تحويل الفضاء السيبراني، إلى مجال خصب للتهديدات والمخاطر، التي تقوض الأمن والسلم الدوليين.

ويبقى ان أهم القواعد الرادعة، هي إعلان مسؤولية الدول عن الاعتداءات التي تنطلق من الاراضي الخاضعة لسيادتها، أو لسيطرتها الفعلية، سواء اصدرت عن أفراد، أو عن اجهزة رسمية لديها، وتطبيق قواعد القانون الدولي الخاص بالنزاعات المسلحة. وعلى ضوء الصعوبات التي يواجهها الوصول إلى اتفاقات دولية حول حماية الفضاء السيبراني، لا بد للدول من العمل على تعبيد الطريق لذلك، عبر الاتفاق على ضرورة بناء الثقة في هذا الفضاء. ويمكن في هذا المجال، الاتفاق على حدود معينة، لا يجوز للدول تجاوزها، ما يمكن ان يؤثر ايجابا في ردعها \عن التصرف نتيجة حسابات خاطئة، تعزز حظوظ نشوب حرب. يضاف إلى ذلك، التزام الدول بمبادئ الشفافية، وتبادل المعلومات حول التهديدات والمخاطر، وإيجاد نموذج حوكمة يواكب طبيعة الانترنت ومخاطرها، يؤمن ارساء قواعد تصرفات مسؤولة. فالأمن السيبراني، شديد الارتباط بمسألة حوكمة الانترنت، وبمسائل سيادة الدول، بحيث لا يمكن الحديث عن تدني متطلبات السيادة في الفضاء السيبراني، عن تلك التي تقر للدول، على اقليمها البري، البحري والجوي.

[47] *The Ikeja High Court Thursday sentenced Nwagbogwu Stephen, 22, to 12 months imprisonment without option of fine for Internet fraud". www.Thetidenews.com.*

٦ . طبيعة الأخطار

مما لا شك فيه، ان تكنولوجيا المعلومات والاتصالات، تتيح امكانات هائلة، وغير مسبوقة، لإنتاجية أفضل في جميع القطاعات، وللتواصل عبر القارات. الا ان البنية التحتية لهذه التقنيات، تمثل ارتباطا بين مصالح متعددة، وخدمات مختلفة، وبلدان عديدة، الامر الذي يجعل من الأخطار في المجال السيبراني، أخطارا عالمية، تطاول الجميع دون استثناء، وتفترض منهم التزاما، بكل ما يضمن أمن تقنيات المعلومات والاتصالات. فلا يمكن لاية جهة، ان تضمن بقائها في منأى عن الأخطار، ما دامت سلامة الآخرين معرضة. فالطبيعة العالمية، تستلزم ردا ذا أبعاد عالمية، تتجاور فيه وتتداخل السياسة، والاقتصاد، والاجتماع، والتقنية، والقانون. هذا عدا عن التعقيدات الناشئة، عما يرتبه خضوع البنية التحتية الأساسية، للقطاع الخاص، وليس لسيطرة الحكومة، اضافة إلى ان القدرات والخبرات، في مجال تقنيات المعلومات والاتصالات، انما تنمو وتزدهر فيه، وتخضع لقوانين السوق. هذا، فضلا عن صعوبة تحديد مصدر الهجوم أو الاختراق، بعيدا عن تبادل المعلومات، والتنسيق بين جهات متعددة، داخلية وخارجية. ففي الفضاء السيبراني، « مجهولة الهوية» هي القاعدة، في الوقت الذي يحتاج فيه بناء الثقة، إلى تحديد الهوية، ومعرفة المصدر، وامكانية الاثبات، الامر الذي لا يمكن تحقيقه، بعيدا عن تضافر جهود جهات متعددة، من القطاعين العام والخاص.

أ- الأخطار القانونية

وتتمثل المخاطر القانونية، بشكل أساسي، في غياب الإطارين التشريعي والتنظيمي، المناسبين للتعامل مع نتائج الأعمال القانونية، وغير القانونية منها، التي تتم في الفضاء السيبراني. فالنشاط الاقتصادي، والتجاري، وغيره، يتطلب تحديدا واضحا، للموجبات والحقوق، بما يضمن معالجة الخلافات الناشئة عنه، بشكل يساهم في تعزيز الثقة بقدرات تكنولوجيا المعلومات والاتصالات، في مجال الخدمات، والتبادل بكل اشكاله وأنواعه. فمستخدمو هذه التقنيات، والمعتمدون على الفرص المتاحة عبر الفضاء السيبراني، بحاجة إلى إطار، يؤمن حماية استخدامهم هذا، وحماية وجودهم في هذا الفضاء، حيث تنتقل أموالهم وبياناتهم.

من هذا المنطلق، تتمثل المخاطر القانونية، في غياب الأمن القانوني، أو حتى في تناقض وتنازع الأنظمة القانونية، من جهة اولى، وفي اتساع امكانات نشوء جنات للجريمة السيبرانية، من جهة ثانية. ويرتفع منسوب هذه المخاطر، مع انعدام التعاون بين البلدان المختلفة، أو حتى مع وجود تعاون، لا يضمن ملاحقة فاعلة، تتلاءم وطبيعة الأعمال والجرائم والاعتداءات السيبرانية، العابرة للحدود، وللانظمة القانونية، والتي لا يقف توسعها على المستوى الجغرافي؛ بحيث تطاول اي مواطن في اي بقعة من الأرض، بل يتعداها إلى توسعها على المستوى الموضوعي، بما يطاول الدول، وامنها، واستقرارها.

ب- الأخطار التقنية

ترافق طبيعة التقنيات والاتصالات، مع أخطار خاصة، مرتبطة بهندستها الخاصة، وبالبيئة التي تعمل في إطارها، اي الفضاء السيبراني. وإذا كانت التقنية، والهندسة، والرقمنة، تتحكم بتوسع تقنيات

المعلومات والاتصالات، وبالولوج إلى الفضاء السيبراني، ورسم حدوده، بما جعل البعض يعتبرونها، قادرة على لعب دور القانون، في تنظيم الفضاء السيبراني، وضبط الأعمال المخلة بأمنه، وصولا إلى إنكارهم على المشرع، حق الاضطلاع بمهمة هذا التنظيم، ففي ذلك ابتعاد عن جادة الصواب.

فقد أثبتت هذه التقنية، انها ليست قادرة على ضبط التصرف الانساني، وتأمين سلامة الأفراد، والمؤسسات والدول، التي أصبحت أكثر اعتمادا عليها. وعليه، دقت أكثر الدول تقدما، ناقوس الخطر، وعلى أكثر من منبر عالمي، للفت الانتباه إلى هشاشة الوضع، والى الخلل العضوي الذي يطال البرمجيات والتجهيزات، على السواء، والذي يشكل نقاط ضعف، يمكن استغلالها بسهولة من قبل الخبراء، في خرق الأنظمة المعلوماتية، والى حجم المخاطر التي يرتبها هذا الامر.

وإذا كان صحيحا ان الحلول التقنية موجودة، فإن الصحيح أيضا، أنها حلول قاصرة، كونها لا تستطيع مواكبة الدينامية التي توجدها، كما لا تستطيع مواكبة التحولات المستمرة، في طبيعة المخاطر. فهي تتبع بروز المشكلة، وتشكل بالتالي، ردا محدودا الزمان والمكان، كما وبمسألة معينة. هذا عدا عن مهارات المتسللين إلى الأنظمة والمخربين، وتعدد الجهات المعنية بالأمن السيبراني (تقنيين، مستثمرين، عملاء، مهندسين، مطوري برامج وتطبيقات...)، وانعكاس ذلك، تعقيدات على مستوى الرؤية، والفهم الجامع للمخاطر، كما للتدابير المفروض اتخاذها. ولا يغفل عن بالنا، حاجة تقنيات الحماية نفسها، إلى الحماية.

من هنا القول، بأن الركون إلى الحلول التقنية، هو ركون إلى المجهول، لاسيما مع صعوبة التحكم بهذه التقنيات، ومع الاعطال التي يمكن ان تطرأ عليها، هذا عدا عن العيوب الخفية التي تعتريها، والتي لا يمكن اكتشافها، الا بعد وضعها قيد العمل. ويأتي في هذا السياق، ما توفره من امكانيات الحركة بطريقة سرية، وان بدرجة نسبية. لكن الإقرار بقصور التقنية، لا يعني عدم الالتفات إلى تطوير آليات الحماية التقنية، والاستعانة بالبرامج والتطبيقات الخاصة، بمنع الولوج إلى البنى التحتية، والى الأنظمة المعلوماتية، لمن ليس له الحق في ذلك، وذلك من خلال تدابير تقنية، ترتكز إلى إدارة الهوية الإلكترونية، واستخدام برامج الحماية من الفيروسات، وبروتوكولات التشفير، وغيرها.

ـ البرمجيات الضارة والسلوكيات الجرمية

يشكل اهتمام بعض الشركات بالتسويق لمنتجاتها على الانترنت، عاملا اضافيا لتعريض الانترنت، والشبكات للعديد من المخاطر، لاسيما منها، تلك التي يمكن ان تنتج عن زرع أنواع معينة من الديدان، أو من الفيروسات، واحصنة طروادة، التي تتخطى برامج الحماية، سواء من خلال البريد الإلكتروني، أو مواقع محركات البحث، والإعلانات، التي تنشر عبرها.

ولعل أخطر ما في الامر، هو تلاقي الافعال والتقنيات، مع النيات الجرمية. ففي تقرير[48] حول اتجاهات أمن الانترنت، نشرته جريدة الرياض، كشف عن علاقة بين بعض المواقع التي تستغلها البرمجيات الضارة، ومجموعة من شركات تسويق، لأدوية غير قانونية.

[48] *www.alriyadh.com/2008/09/03/articles371725*
تقرير اتجاهات أمن الانترنت ٢٠٠٨ يكشف عن صلة بين مواقع إلكترونية مستغلة من برمجيات ضارة وسلسلة توريد ادوية غير قانونية عبر الانترنت

وعن واقعة تؤشر إلى اهمية الأمن في الفضاء السيبيري، نشرت جريدة العرب بتاريخ ٢٠٠٨/٨/٢٠ خبرا بعنوان: «الإرهابيون الجدد...قراصنة انترنت». وقد جاء في تفاصيله، سرد لتحذيرات خبراء في مجال الانترنت، من ان الهجوم الإرهابي القادم على الولايات المتحدة الأميركية، ربما يكون من قبل قراصنة الانترنت. وقد أبرزوا خشيتهم هذه، نتيجة الهجوم الذي شنته روسيا، قبل اعتدائها على جورجيا، على جميع المواقع الرسمية الجورجية، على الانترنت.

ويزداد الامر سوءا، مع التخصص الذي يبدو واضحا في مجال اختراق الأنظمة والشبكات، ومع ديمقراطية نشر المعرفة، التي تبدو في أحسن تجلياتها، مع المواقع التي تؤمن برمجيات متخصصة في الاختراق، يمكن الحصول عليها مجانا ودون مقابل. وتقوم هذه المواقع، بدراسة كل نظام على حدة، انطلاقا من خصائصه، ومن الميزات الخاصة بإدارة حمايته. ذلك ان ما يعني مديري النظام، والمتخصصين بحمايته، هو نفسه الذي يعني مقتحمي الأنظمة. كما يمكن الحصول، من هذه المواقع أيضا، على التعليمات الخاصة، بنقاط الضعف في الأنظمة، وبمواقع الاختراق الممكنة، وبأساليب تنفيذ العمليات بطريقة مهنية، وتقنية عالية.

ومع انتشار الاتصالات اللاسلكية، وتوسع استعمالاتها في الأنظمة، يتسع عدد ونوع البرمجيات[49]، كما يتسع حجم مساحات وامكانات الاختراق،بحيث تتوزع هذه الاخيرة، على كل نقاط النفاذ، إلى خدمات الاتصال، بشكل يستدعي احتياطا وحذرا دائمين [50].

وتعمل البرامج التي تستعمل في عمليات الاقتحام والاختراق، عبر تقنيات متعددة ومختلفة، منها على سبيل المثال: اكتشاف الشبكة، ومسح المعلومات المتوفرة عليها، كما الأجهزة المتصلة بها والمستخدمة عليها، كشف أنواع التشفير، إنشاء ملفات خاصة بكل شبكة وتحديد طريقة الاتصال بها، وفك الشيفرة المستخدمة.

ـ تقنيات تهدد الانترنت (برامج متخصصة في نشر الفيروسات)

تعتبر التقنيات المستخدمة على الانترنت، المصدر الأول للتهديدات التي يمكن أن تواجهها هذه الاخيرة، كونها تحمل في طبيعتها، البذور المؤاتية لذلك، سواء عبر نقاط الضعف التي تعتريها، أو عبر البرامج المتخصصة في نشر الفيروسات، وزرع أدوات التجسس على المواقع والأجهزة، ما يفتح المجال واسعا، لاستخدام التكنولوجيا في الانشطة التخريبية والجرمية، التي تطال الانترنت، كما تطال الأفراد والمؤسسات.

فالبريد الإلكتروني مثلا، وهو أكثر تطبيقات الانترنت استخداما، يشكل هدفا سهلا، لمن لديه محلل بروتوكولات، وقدرة على الوصول إلى أجهزة الروتر Routers ، والأجهزة الشبكية الأخرى التي تعالج الرسائل التي يتولى نقلها، وذلك أثناء عملية الانتقال، من شبكة إلى أخرى، اذ يمكن للمتسل أن يعترض الرسائل، فيقرأ أو يغيّر محتواها.

[49] *Examples of some programs: Kismet for Linux.Netstumbler for windows.Netdiscover for nets not using DHCP.WIFI RADAR. AirSnort, AirCrack.Cowpatty.*
[50] *Thomas.M..Thomas.Wireless security, InformIT. http://www.informit.com/articles/article.aspx?p=177383&seqNum=7 Wireless networking is everywhere! That is not meant as hyperbole—it really is everywhere. Wireless technology uses radio waves to transmit data, so wireless packets are probably flowing in the air in front of you as you read this.*

كذلك، تعتبر الشبكات حاملة لخطر مستمر، نتيجة تكاثر الفيروسات في الفضاء السيبيري[51] ، حيث يشهد عالم الانترنت، بروز فيروسات جديدة، بشكل يومي، ومتواصل. ويمكن الاستدلال على توسع حركة نشر الفيروسات، من خلال ما تنشره المواقع المتخصصة، مثل Symantec و MCafee، ومن خلال انتشار برامج الحماية نفسها، والسياسات المعتمدة في تيويمها، وتحديثها، دون انقطاع، عبر الانترنت. ولا ينحصر منتجو الفيروسات، والبرامج التي تعرض أمن الانترنت، في منطقة جغرافية واحدة، بل أنهم يتوزعون على العديد من الدول [52].

ويأتي في عداد هذه البرامج، ما يعرف بالadware[53]، والspyware، والMalware[54]، والZombie[55]. وهذه الاخيرة، برامج تدخل الأجهزة بواسطة ما يعرف بالدودة المعلوماتية[56]، وتتميز عن الفيروس، في كونها تنتشر، دون حاجة إلى أي خطوة من قبل مستخدم الكومبيوتر، كفتح ملف ما، أو الضغط على وصلة معينة. وتظل الworm، في ثبات داخل الجهاز المقتحم، إلى أن تتلقى أمرا، أو حتى تاريخ معين. وغالبا ما يتم زرع الدودة، على أعداد كبيرة من الأجهزة، حيث تتم برمجتها، لتعمل بالتزامن مع بعضها البعض، ما يحرك أعدادا كبيرة من أجهزة الكومبيوتر في العالم، دفعة واحدة، لتنفيذ مهمة واحدة، كارسال رسائل بريدية، أو أوامر بحث إلى محرك معين، أو طلبات دخول إلى مواقع معينة.

فتتحول الأجهزة المقتحمة، إلى أداة تستخدم في الاعتداء، الذي يعرف ب "منع الخدمات"[57]، وذلك عندما تنفذ الامر المعطى لها بالاتصال. ويعتبر هذا النوع من الاعتداء، خاصا إلى حد ما، بالمواقع التي تتعاطى الانشطة التجارية، ما يفسر انتشاره وخطورته، بالنسبة للبلدان الأكثر تقدما في هذا المجال. وتأتي في طليعة هذه البلدان، الولايات المتحدة الأميركية، وانكلترا، وفرنسا، واليابان والصين والمانيا. ولا يتوانى بعض رجال الأعمال، عن اللجوء إلى خدمات مقتحمي البرامج، للاضرار بمصالح منافسيهم. ففي آذار (مارس) من العام ٢٠٠٥، تمكن مكتب التحقيقات الفدرالي، في الولايات المتحدة الأميركية، من توقيف أحد المقتحمين، اضافة إلى رجل الأعمال الذي استخدمه، لمهاجمة موقع شركة منافسة. وقد استمرت هذه العمليات، لمدة خمسة أشهر، وتسببت بحوالي مليوني دولار أميركي من الخسائر، للمنافس، كما لعدد من الشركات، التي تستخدم نفس الISP[58].

---

[51] *Le virus: Programme informatique d'autoréplication, doté de fonctions nuisibles, qui s'installe en annexe d'un programme ou fichier hôte pour se propager.Rapport semestriel de MMELANI 2006/II (Juillet a decembre).*

[52] *SoBig virus from Moscow (summer 2003), which came in many variants. The sixth one was so successful that Microsoft together with Interpol and FBI set up a system of reward ($250,000) for information leading to the author(s). I love you virus from Philippines (2002), Code Red a worm from China (2003).*

[53] *Les «adware», terme issu de la contraction des mots anglais «advertising» (publicité) et «software», s'utilisent fréquemment à des fins publicitaires. Ils enregistrent les habitudes de surf de l'utilisateur pour lui offrir ensuite les produits correspondants (p. ex. via des liens). Rapport semestriel de MMELANI 2006/II (Juillet adecembre).*

[54] *Malware: "Programme malveillant / maliciel. Le terme anglais «malware» est la contraction de «malicious» et de «software». Terme générique employé pour tout logiciel exécutant des fonctions nuisibles sur un ordinateur (comme p.ex. les virus, les vers ou les chevaux de Troie). Rapport semestriel de MMELANI 2006/II (Juillet a décembre).*

[55] *Réseau de zombies : « Réseau d'ordinateurs infectés par des programmes malveillants (bots). Un pirate (le propriétaire du réseau de zombies) les contrôle complètement à distance. Un réseau de zombies peut compter de quelques centaines à des millions d'ordinateurs compromise", rapport semestriel MELANI 2006/II (juillet a décembre) .*

[56] *Le ver : « A la différence des virus, les vers n'ont pas besoin de programme hôte pour se reproduire. Ils utilisent les lacunes de sécurité ou des erreurs de configuration des systèmes d'exploitation ou des applications, pour se propager d'ordinateur en ordinateur", rapport semestriel MELANI 2006/II (juilet a decembre)>*

[57] *Zombies participate to Distributed Denial of Service attacks (DDOS)*

[58] *McAfee virtual criminal report: North American Study into Organised Crime and the Internet, 2005, p:11 "The Case of the Hired Hacker".*

أما برامج التجسس الSpyware[59]، فهي البرامج التي تتولى تسجيل حركة مستخدم الانترنت، خدمة لطرف ثالث. وغالبا ما يكون الهدف الكامن وراء ذلك، تجاريا، حيث يعتبر الربح المادي، من أهم الدوافع وراء ممارسة هذه الاعتداءات[60]، وتعتبر المواقع الإباحية في هذا المجال، مواقعا خطرة، كون ٨٠٪ منها، تحمل برامج تجسس، على الأجهزة التي تتصل بها [61].

وتزيد هذه الخطورة بالنسبة للشركات، على ما يبدو، مع استخدام البرامج ذات المصادر المفتوحة، كما نبه إلى ذلك، بعض الاختصاصين[62]، كونه يعرض سلامة شبكات الشركات، وموظفيها، وزبائنها للخطر، الذي ينتج عن إزالة الحواجز التقليدية، التي تستخدم في البرامج المرخصة، والتي حافظت على سلامتها، حتى اليوم.

كما لفت الاختصاصيون، في معرض التعليق على الحماسة التي كان يبديها البعض، فيما يتعلق باستخدام الweb ٢,٠s‘، إلى ما يمكن أن يقوم به الhackers and spammers ، من وضع بعض الفيروسات والworms، على صفحاتهم الخاصة،بما يعرض سلامة الأنظمة والبرامج، التي يستخدمها أفراد مواقع الشبكات الاجتماعية[63]، التي ينتمون اليها، على الانترنت، ومنهم الموظفون، والعاملون في الشركات، والمؤسسات العامة والخاصة.

ويعتبر هذا التهديد، شديد الجدية والخطورة، اذا ما أضفنا اليه واقعا جديدا، ألا وهو توجه الجريمة المنظمة، نحو الاستثمار في الجرائم السيبيرية، كمصدر جديد للعائدات، والمردود الذي يمكن اعادة توظيفه، في توسيع دائرة النشاط الجرمي، وتعزيزه[64].

ـ (الدودة "كونفيكر": استغلال ثغرات البرامج)

في اكتوبر (تشرين الأول) من العام ٢٠٠٨، وزعت مايكروسوفت تحذيرا مضمونه، ان ثغرة في المخدم، تسمح بتنفيذ أحد الرموز، على عدد من انظمة التشغيل لديها، دون المرور بعملية التحقق منه، عبر استخدام عدد من التقنيات والتعليمات المعقدة، لتضليل نظام الحماية على الجهاز، ومنع برامج مكافحة الفيروسات، من مكافحتها. كذلك، فقد حذرت من ان هذه الثغرة، يمكنها ان تحول الجهاز، إلى وسيلة اعتداء على الشبكات والأجهزة الاخرى، فيما لو تلقت أمرا عن بعد، بواسطة ما يعرف ببروتوكول الاتصال من بعيد، RPC. كما يمكن ان تستغل في خلق دودة تستخدم النظام.

[59] *Spyware collecte des informations, à l'insu de l'utilisateur, sur ses habitudes en matière de navigation (surf) ou sur les paramètres du système utilisé pour les transmettre à une adresse courriel prédéfinie » rapport semestriel MELANI 2006/II (juillet a décembre). Ces logiciels espions qui observent l'internaute, www.LeMonde.fr. 06.06.07. le logiciel espion (en anglais, spyware) s'installe dans un ordinateur dans le but de collecter et de transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance.»*

[60] *http://www.sophos.fr/sophos/docs/fra/comviru/viru_bfr.pdf.*

[61] *JeromeSaiz « 80% des sites pornographiques seraient infectieux » http://www.lesnouvelles.net/articles/chiffres/675-sites-pornographiques-et-spywares.html.*

[62] *Larry Greenmeier, Sharon Gaudin, Information Week. http://www.informationweek.com/story/showArticle.jhtml?articleID=199702353*
- Kris Lamb, director of IBM Internet Security Systems division's X-Force security research organization.
- David Cole, director of Symantec Security Response.
- Paul Judge, CTO at security vendor Secure Computing.

[63] *Tech Encyclopedia. http://www.techweb.com/encyclopedia social networking site. A web site that provides a virtual community for people interested in a particular subject or just "hang out" together.*

[64] *Federal Prosecutor: Cybercrime Is Funding Organized Crime,JULY 20, 2007, "Assistant U.S. Attorney Erez Liebermann, chief of the computer hacking and intellectual property section in New Jersey›s U.S. Attorney›s Office, says cybercrime has been so profitable for organized crime that they›re now using it to fund the rest of their underground operations". http://www.darkreading.com/document.asp?doc_id=129608&WT.svl=cmpnews1_1*

وقد تم اعتبار هذه الثغرة، على احد المواقع المتخصصة[65]، من الأشد خطورة، اذ حصلت على تقييم ١٠ على عشرة. وبالفعل، فقد انتشرت نتيجة لذلك، دودوة أطلق عليها اسم «كونفيكر»، Conficker، سريعا عبر الأجهزة، وبواسطة وسيلة التخزين، الUSB. ومن آثار هذه الدودة، انها تمنع المستخدم من الدخول إلى حسابه، أو إلى عدد من المواقع، في طليعتها تلك الخاصة ببرامج مكافحة الفيروسات، واغلاق الحسابات على المخدمات، اضافة إلى ابطاء عمل النظام. وتعتبر الميزة الأساسية لهذه الدودة، قدرتها على اخفاء أثرها، ما جعل مكافحتها شبه مستحيلة، حيث صعبت ازالتها من النظام، ما يعني وجود عدد ضخم من الأجهزة، التي يمكن توجيهها في عملية روبوتات تخريبية، يمكن للمجرمين، والمعتدين السيبرانيين، استخدامها.

في الواقع، تعمل هذه الدودة، على خلق شبكة من الاتصالات بين مختلف الأجهزة المصابة، عبر عدد من أسماء النطاقات والمواقع، ما يمنع اثبات تبعة الاعتداء أو منشئه. اذ يمكن لجهة اجنبية، تسخير مخدمات بلد معين، لتنفيذ اعتداءات، على أنظمة ومواقع بلدان أخرى، واظهار الامر، كانه صادر فعلا من هذه المخدمات[66].

وفي مواجهة هذه التهديدات، يمكن لمستخدمي الانترنت، ومقدمي خدمات المعلومات، أن يلعبوا دورا، لا بأس به، في تأمين حد معين من الحماية للأنظمة، كما للمعلومات والبيانات. وذلك، من خلال استخدامهم برامج مكافحة الفيروسات، وتقنيات خاصة، تمنع اقتحام قواعد المعلومات، وتشويهها، أو التلاعب بها، اضافة إلى اتخاذهم التدابير، التي تمنع تلفها، أو ضياعها، مثل: البصمة في الرسالة الإلكترونية، والتشفير، والاحتفاظ بنسخ يمكن استرجاعها عند تلف البيانات، لاي سبب كان.

كما يمكن، في مجال أمن المعلومات والأنظمة، اللجوء إلى التحقق من هوية الاشخاص، والاطراف المتصلة، من خلال كلمات المرور، والشهادات الرقمية، التي يصدق عليها من طرف ثالث، اضافة إلى الجدار الناري[67]، الذي يمنع عمليات الولوج، غير المسموح به.

[65] *https://cve.mitre.org/*
[66] *Chinese Hackers Use US Servers In Cyber Attacks. http://freebeacon.com/national-security/chinese-hackers-use-us-servers-in-cyber-attacks/*
[67] *fire wall*

٧. الاستخدام المتنامي والكلفة الباهظة

في العام ١٩٩٣ كان عدد المواقع الإلكترونية لا يتجاوز الخمسين موقعا، بينما تجاوز اليوم حدود المليار موقع[68]، ومن المتوقع أيضا، تصاعد هذا العدد خلال الأعوام القادمة.

على خط مواز، يتوقع الخبراء تزايد عدد الأجهزة المتصلة بالانترنت، في العام ٢٠٢٠، إلى ما يقارب المليارين، وذلك، في مقابل عدم اتقان مستخدميها لأساليب وطرق حمايتها، حتى في حال وجود برامج مكافحة الفيروسات والبرامج الخبيثة، والاختراقات[69].

في مقابل هذه التطورات السريعة، تبقى الاحاطة صعبة ومعقدة، بالعديد من الجوانب السياسية، والاقتصادية، والقانونية والاجتماعية. الا ان هنالك اجماعا دوليا، على الحاجة إلى مقاربة لا تطال فقط تحديد المخاطر، والتهديدات، والردود المناسبة، بل تطال إلى جانب ذلك، حقوق الأفراد والدول، في المجال السيبراني، ومستقبل حوكمة الانترنت، ودور المجتمع المدني، والحكومات، والأجهزة الأمنية، في حماية هذه الحقوق وهذا الفضاء. فمع الاعتماد المتصاعد، وشبه الشامل، على تقنيات المعلومات والاتصالات، تأتي مخاطر جدية، وكلفة عالية، لا بد من ان تترك آثارها، على الأمن القومي، والدولي.

وتشير التقارير الموضوعة من الجهات المتخصصة، في مجال مكافحة الاعتداءات على الأنظمة المعلوماتية، إلى تصاعد في وتيرة الاختراقات، وسرقة البيانات، والاعداد اليومية للاعمال الجرمية السيبرانية، وملايين البرامج الخبيثة، التي تستعمل في ارتكاب الأعمال غير الشرعية، ضد المواقع، والاصول، والأفراد على الانترنت[70].

فلقد شهد العام ٢٠١٥، التأكيد على عدد مما اصبح مسلمات، كالقيمة الاقتصادية العالية للبيانات ذات الطابع الشخصي، وعدم حصانة أي مؤسسة، اينما كانت، في القطاعين العام أو الخاص، ضد الاعتداءات السيبرانية، وعدم وجود قطاع غير مستهدف [71]. كما أكدت على ان المجرمين السيبرانيين، يزدادون اتقانا للأساليب الاعتداء، ويصبحون أكثر تنظيما. كذلك برزت منظمات إجرامية جديدة، مثل DD4BC gang[72]، التي اشتهرت بهذا النوع من الاعتداءات، أو بالتهديد به، مقابل فدية تدفعها الشركات المستهدفة. أنشئت هذه العصابة بداية، كما يؤشر اليه اسمها، لتوزيع اعتداءات تعطيل الخدمة، واقفال المواقع، بهدف سرقة الBit coins ، لكنها سرعان ما وسعت نشاطاتها، لمهاجمة مواقع الميسر والكازينوهات، ومن ثم، بدأت باستهداف شركات مالية تقليدية، منتشرة حول العالم، في أوروبا، واستراليا، وأميركا.

[68] *http://www.internetlivestats.com/total-number-of-websites/*
[69] *McAfee Labs Report 2016 Threats Predictions. Devices will continue to grow in volume and variety, and the forecast for connected devices by 2020 is now 200 billion and climbing. Combine this massive increase in the number of devices that need to be secured with a well-documented shortage of security talent, and it is easy to understand why the security industry must simplify and automate defenses and their configurations, and improve efficiency with machine learning and networked collaboration. Even with those improvements, security settings will remain well outside the realm of the average person, fueling the growth in security services that will provide education, guidance, setup, and update assistance to consumers and small businesses. People who install home and small business networks will be required to get much better about providing secure systems to their customers, because no one is going to be the security administrator on these networks. - http://www.mcafee.com/tw/resources/reports/rp-threats-predictions-2016.pdf*
[70] *http://www.mcafee.com/tw/resources/reports/rp-threats-predictions-2016.pdf*
[71] *http://www.computerweekly.com/news/4500258027/No-sensible-business-ignoring-cyber-threats-says-Kemp-Little. "The potential business impacts [of cyber attacks] combined with increasing levels of awareness among consumers mean that no sensible business is still ignoring this threat," said Nicola Fulford, head of data protection and member of the cross-departmental cyber security team at Kemp Little.*
[72] *DDoS for Bitcoin*

وتأتي في مقدم المؤسسات التي تعرضت للهجمات في هذا العام، المكتب الأميركي لإدارة الموارد البشرية، وموقع "آشلي ماديسون"، وسلسلة من الفنادق: كالهيلتون وترامب، وشركة الاتصالات TalkTalk، اضافة إلى مصنع الالعاب VTech.

في المقابل، شهد هذا العام، تعاونا أكبر بين الأجهزة الأمنية، حول العالم، في تصميم على مواجهة الاعتداءات السيبرانية، وشل البنية التحتية لها، كانت نتيجتها، توقيف العديد من المجرمين السيبرانيين. كما اهتمت السلطات، والقطاعات، المعنية بالأمن، كخبراء الأمن، ومصنعي برامج الحماية، بتوجيه عدد من التوصيات، إلى الشركات بشكل خاص، لمقاربة الحماية والدفاع في وجه الهجمات السيبرانية، على قاعدة المخاطر، وللانتباه إلى عمليات الاختطاف المعلوماتي، وطلب الفدية. وتتم هذه العمليات، باستخدام برامج تشفير خبيثة، تحتجز المعلومات عبر تشفيرها، ومنع الوصول اليها، الا بعد دفع الفدية. وكانت عمليات تعطيل الخدمة، distributed denial of service (DDoS) attacks الأكثر رواجا، قد سعت إلى تشتيت انتباه المسؤولين عن أمن الأنظمة، بشكل أساسي.

وقد قدر متوسط كلفة الخسائر المترتبة على الاعتداءات السيبرانية، على المؤسسات الكبيرة في بريطانيا، بما يعادل ٣,١٤ مليون جنيه استرليني[73]، بينما ارتفعت نسبة وقوع الاعتداءات، والكلفة الاقتصادية إلى الضعف، مقارنة بالعام ٢٠١٤. كذلك، تم نشر بيانات حساسة، سرقت من موقع آشلي ماديسون، وبعض المواقع الاخرى المرتبطة بها، بعد توجيه طلبات إلى الشركة مالكة الموقع، باقفاله. بينما تسربت بيانات ملايين الاهل والاطفال، من الاعتداء على VTECH. كما كشف، خلال هذا العام، العديد من شبكات التجسس المنظم. وكانت منظمة FireEye، المتخصصة في الأمن السيبراني، قد اتهمت الحكومة الصينية، بقيادة عملية تجسس واسعة، منذ عشر سنوات، بهدف سرقة البيانات الحساسة، لمنظمات ومؤسسات، شرق أوسطية وآسيوية. كذلك، أعلنت السلطات الأميركية، توقيف عدد من المشتبه بهم، في قضية تجسس تجاري[74]، في عملية كانت تهدف إلى سرقة بيانات حساسة، من خدمات وكالات الانباء.

وقد تمكن عدد من الدول، خلال عملية مشتركة، بين أجهزة الأمن، وأجهزة الأمن السيبرانية المتخصصة، وعدد من المنظمات الخاصة، من تفكيك مجموعة من الروبوتات Dorkbot botnet[75]، كما تمكن عدد من الوكالات الأوروبية، من اقفال عدد من الخوادم، التي كانت تستخدم روبوتات، تستهدف سرقة البيانات الشخصية والمصرفية[76]. كما تم توقيف مئة وثلاثين شخصا، على علاقة بعمليات خداع سيبرانية، في عشرات المطارات، حول العالم [77]. وفي السياق عينه، أعلن الأوروبول، عن إمكانات جديدة، لمحاربة الإرهاب والجريمة السيبرانية[78].

[73] *2015 Information security breaches survey. http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html*

[74] *Nine Charged in Insider Trading Case Tied to Hackers. Paul J. Fishman, the United States attorney for New Jersey, said that nine people were charged after stealing corporate news releases and using the information to make over $100 million. By THE ASSOCIATED PRESS on Publish DateAugust 11, 2015. Photo by Karsten Moran for The New York Times. Watch in Times Video http://www.nytimes.com/2015/08/12/business/dealbook/insider-trading-sec-hacking-case.html?_r=0*

[75] *http://www.welivesecurity.com/2015/12/03/news-from-the-dorkside-dorkbot-botnet-disrupted/. News from the Dorkside: Dorkbot botnet disrupted*

[76] *National Crime Agency disables Ramnit bank-robbing botnet. http://www.computerweekly.com/news/2240241226/National-Crime-Agency-disables-Ramnit-bank-robbing-botnet*

[77] *http://www.computerweekly.com/news/4500248925/Police-arrest-130-in-global-anti-cyber-fraud-operation. Police arrest 130 in global anti-cyber fraud operation*

[78] *Europol: deal on new powers to step up EU police cooperation and fight terrorism. http://www.europarl.europa.eu/news/en/news-room/20151130IPR05456/Europol-deal-on-new-powers-to-step-up-EU-police-cooperation-and-fight-terrorism*

٨. في الوقاية والتمكين

مع ازدياد النشاط التجاري، والمالي، يزداد حجم دفق البيانات والمعلومات، عبر الشبكة العالمية للمعلومات، وتتوسع حركة المبادلات التجارية، والتحويلات المالية على الانترنت[79]. في المقابل، تتسع حركة التشريع والتنظيم، في البلدان التي تعي أهمية اقتصاد الانترنت، حول مسائل: حماية المستهلك، وحماية البيانات، وسلامة التحويلات، والسلطات القضائية المختصة، وحماية الملكية الفكرية، والخصوصية، وغيرها الكثير مما يتعلق بالمسؤولية عن الخدمات، ونوعيتها.

وتبرز في هذا المجال أيضا: القضايا المتعلقة بحوكمة الانترنت، والحماية من الجريمة السيبرانية وتداعياتها، على تطور المعاملات الإلكترونية، واستخدام تقنيات المعلومات والاتصالات. ومن المتوقع في هذا المجال، بروز القضايا التي ترتبط باستخدام المال الإلكتروني، أو المال الجوال[80]، وطرق الدفع الأمنة، وآلياته، وتخزين المال الإلكتروني، واستخدامه كبطاقات دفع افتراضية، أو كبطاقات هدايا. ويضاف إلى ذلك، ازدياد نزاعات العمل، التي يمكن ان تنشأ في إطار نماذج العمل عن بعد، واستخدام تقنيات المعلومات والاتصالات، كما الشبكات الاجتماعية، والشبكات الداخلية، في اماكن العمل. وتندرج هنا أيضا، قضايا حماية خصوصية العامل، وحقوقه.

وتبذل الهيئات الدولية، وفي مقدمها الاتحاد الدولي للاتصالات، جهودا حثيثة ، تؤكد على حتمية الأمن السيبراني، حيث خصصله، جزءً أساسياً من برامجه، وخطط عمله المختلفة[81].

وقد تعاملت الأمم المتحدة، مع تقنيات المعلومات والاتصالات، لاسيما فيما يتعلق بالانترنت، من منطلق كونها أداة للتنمية الاجتماعية والاقتصادية[82]، ووسيلة ناجعة في السعي إلى تحقيق أهداف الالفية. وعليه، فقد اوكلت إلى المجلس الاقتصادي الاجتماعي، متابعة قضايا التنمية المتعلقة بالانترنت. في المقابل، تهتم اللجنة الخاصة بالعدالة الجنائية ومنع الجريمة، الموكلة بمتابعة الجهود الدولية في مكافحة ومنع الجرائم الوطنية والعابرة للحدود[83]، بالقضايا المتعلقة بجرائم الانترنت.

وفي السياق عينه، هنالك تعاون بين المكتب المعني بالمخدرات والجريمة (UNDOC) في الأمم المتحدة، والاتحاد الدولي للاتصالات، لمساعدة الدول الأعضاء في الاتحاد، على الحد من المخاطر التي تشكلها الجريمة السيبرانية، وذلك بموجب مذكرة تفاهم موقعة بين المنظمتين، في منتدى القمة العالمية لمجتمع المعلومات[84].

---

[79] تقرير : 13% زيادة في المبيعات عبر الانترنت في ٢٠١١ - *http://www.al7ll.com/vb/thread22429.html. E-Commerce growing like hell - http://www.brainsins.com/us/blog/ecommerce-growing/1459.* *J.P. Morgan: Global E-Commerce Revenue To Grow By 19 Percent In 2011 To $680B. http://techcrunch.com/2011/01/03/j-p-morgan-global-e-commerce-revenue-to-grow-by-19-percent-in-2011-to-680b/*

[80] *E-money or m-money*

[81] الاتحاد الدولي للاتصالات - دليل الأمن السيبراني للبلدان النامية -2007 الموجزالتنفيذي – «ولذلك كانت إقامة حلول كافية على صعيد الأمن والثقة تمثل واحداً من التحديات الرئيسية التي يتعين أن يعالجها مكتب تنمية الاتصالات في الاتحاد الدولي للاتصالات في متابعة جهوده لمساعدة البلدان على استعمال الاتصالات وتكنولوجيا المعلومات والاتصالات».

[82] *Resolution 60/252,27 April 2006, adopted by the General Assembly- World Summit on the Information Society. "Reaffirming the potential of information and communication technologies as powerful tools to foster socio-economic development and contribute to therealization of the internationally agreed development goals, including the Millennium Development Goals,"*

[83] *Economic and Social Council Resolution 1992/22: Implementation of General Assembly Resolution 46/152 concerning operational activities and coordination in the field of crime prevention and criminal justice, E/1992/92, 30 July 1992.*

[84] *UN and ITU team up to fight Cybercrime By Messaging News staff*

On *May 19, 2011 the ITU , the United Nations agency for information and communications technologies, cemented new global partnerships designed to make cyberspace a safer, more secure place to be for consumers, businesses, and – most crucially – children and youth.*

A *Memorandum of Understanding (MoU), signed between ITU and the United Nations Office on Drugs and Crime (UNODC) at this year's WSIS Forum event in Geneva will see the two organizations collaborate in assisting ITU and UN Member States mitigate the risks posed by cybercrime.*

http://www.messagingnews.com/short-takes/un-and-itu-team-fight-cybercrime

على خط مواز، اتجهت معظم الدول المتقدمة، إلى إقرار سياسات وقائية ودفاعية، ضد الهجمات السيبرانية، وخصصت الدول الكبرى، مثل الولايات المتحدة الأميركية[85]، واستراليا، والمملكة المتحدة، مبالغ طائلة، لمعالجة مسائل الأمن السيبراني، وتأمين استقرار الفضاء السيبراني. وليست هذه الحقيقة، سوى مؤشر، إلى مدى الاهتمام الذي توليه هذه الدول، لارساء الثقة والاستقرار، كما السلامة والأمن، في هذا الفضاء.

فاقتصاد العالم، كما حياتنا اليومية، متصلان اتصالا وثيقا بالفضاء السيبراني. وبالتالي، فان الخدمات الحيوية، كما الأمن، والدفاع، والعلاقات الدولية، مهددة في كل لحظة، نتيجة الاختراقات، والاعتداءات على الشبكة العالمية للمعلومات، وعلى الأنظمة المعلوماتية، وقواعد المعلومات. ولم تتأخر الإدارة الأميركية، عن استحداث قيادة عسكرية جديدة، مختصة بأمن الفضاء السيبراني[86]، تتولى مروحة من النشاطات العسكرية، تشمل إلى الحماية، القيام بمناورات سيبرانية، سواء لتحديد مدى فاعلية الحماية، أو مدى القدرة على الرد، أو للتعرف إلى مكأمن الضعف، والتدريب على آليات الرد . ويتم ذلك، في إطار استراتيجية اعدتها وزارة الدفاع، في العام ٢٠١١، حول كيفية العمل في الفضاء السيبراني[87]. وكان رئيس الوزراء الانكليزي، غوردن براون، قد أعلن هو أيضا، عن إنشاء وحدة خاصة، لمكافحة الجريمة السيبيرانية[88].

ومع بروز الحوسبة السحابية، تستعد الشركات الكبرى، كما الحكومات، لنقلة نوعية، تتمحور حول النماذج الجديدة، في تخزين ومعالجة البيانات والمعلومات، وانتقالها في الفضاء السيبراني، وتواجدها في أماكن بعيدة عن سيطرتها المباشرة. كما تتمحور حول الكلفة، ونوعية الخدمات وسلامة المعلومات. وقد بدأ البعض منها، في وضع بنود على موازنتها، خاصة بالخدمات المرتبطة بهذه التقنية، كما بالسياسات والاستراتيجيات التي لا بد من وضعها، بحيث تؤمن الاطر الصحيحة، وآليات التعاقد، والبنى الادارية الضرورية لذلك.

وكان قادة القطاعات الصناعية والتجارية، قد وجهوا طلبا إلى لجنة الاتحاد الأوروبي، لإيجاد الإطار التشريعي المناسب، لخدمات الحوسبة السحابية[89]. فبعد انتقال الخدمات الكلاسيكية، كالبريد الإلكتروني، والرسائل القصيرة، وشبكات إدارة العمل، إلى الافادة من خدمات الحوسبة السحابية، ستنتقل دون أدنى شك، إدارة المحفظة الإلكترونية، والخدمات المالية والمصرفية، والنشاطات الحكومية، من نقل وموارد طاقة وغيرها. وبالتالي، يصبح ملحا، تقرير الموجبات والحقوق، بما يضمن الانسياب السهل للمعلومات، وتفادي ممارسات مزودي الخدمات، التي تمنحهم ارباحا غير محقة. كما يبدو ضروريا، استيعاب الحاجة إلى مقاربة جديدة لحماية المعلومات، تبعا لحساسيتها، انطلاقا من الاعتماد على المعايير والمقاييس الدولية، في هذا المجال. وهنا أيضا، يطرح المختصون، أهمية سياسات الوصول إلى المعلومات وحماية البيانات، لاسيما مع البلبلة التي ما زالت تتحكم في هذا الموضوع، ومع انعدام

[85] *PricewaterhouseCoopers, Cyber Security M&A: Decoding Deals in the Global Cyber Security Industry (Nov. 2011)*
[86] *Les USA se dotent d'un commandement militaire pour le cyberspace. …porte parole du pentagone : « les risques lies a la cybersecurite figurent parmi les defiseconomiques et de securite nationale les plus serieux du XXIe siecle ». http://www.elwatan.com/Les-USA-se-dotent-d-un*
[87] *www.defense.gov/news/d20110714cyber.pdf.*
[88] *Le cyberspace anglais desormais protégé par d'anciens pirates informtiques. http://techno.branchez-vous.com/actualite/2009/06/le_cyberspace_anglais_desormais*
[89] *EU commission: industry calls for true digital single market in recommendations on European Cloud Strategy.*

الانسجام بين القواعد التشريعية الوطنية. فمع انتقال المعلومات، والعقود الجديدة، ومتطلبات تأمين ونوعية عالية من الخدمات، وصيانة، لا بد من إيجاد نماذج جديدة، تأخذ كل هذه العناصر بعين الاعتبار.

٩. المخاطر السيبرانية: من الطوارئ الدولية

تحولت المخاطر السيبرانية، بما تمثله من تهديد للفرد، والمجتمع، والدولة، إلى مسألة تدرج على لوائح الطوارئ الدولية. وكان الاتحاد الدولي للعلماء، قد ادرجها على لائحة اهتماماته، كواحدة من المسائل، التي لا بد من معالجتها، قبل ان تتحول إلى سبب لاندلاع حروب، ووقوع كوارث[90]، تهدد الانسانية جمعاء، ودون اي تمييز بين الدول المتقدمة تكنولوجيا، أو تلك الأقل تقدما.

وقد قدم الاتحاد، بناء على ذلك، تقريرا في العام ٢٠٠٣، إلى القمة العالمية لمجتمع المعلومات، التي انعقدت في جنيف، بعنوان «نحو نظام عالمي للفضاء السيبراني»، اقترح فيه عددا من التوصيات، جاء فيها:

- حث الأمم المتحدة، على قيادة الجهود بين الحكومات المختلفة، لتأمين عمل وسلامة الفضاء السيبراني، بحيث لا يتحول إلى مرتع للمخاطر، نتيجة استغلال الجريمة له.
- إيجاد قانون شامل للفضاء السيبراني، وتحقيق الانسجام بين التشريعات الوطنية، التي تحكم الجريمة السيبرانية، من خلال نموذج، يمكن ان يكون الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية، ووضع قواعد تعاون دولي، ومساعدة متبادلة، من خلال مراكز الاستجابة لطوارئ الانترنت، والمشاركة في الشبكة المعروفة ب ٢٤/٧، والتي تعمل بشكل متواصل، على رصد حركة الانترنت.
- تطبيق القوانين الدولية، من قبل هيئات متخصصة في الأمم المتحدة، على الاعتداءات السيبرانية، التي يمكنها ان تهدد السلم الدولي، مثل الإرهاب السيبراني، والحرب السيبرانية، والجريمة السيبرانية.
- دراسة السيناريوهات، والمعايير، والعقوبات الدولية، التي يمكن ان تطبق على مرتكبي الاعتداءات.
- دراسة امكانية إنشاء وكالة دولية، تكون لها صلاحية دراسة ومراجعة قواعد السلوك، في الفضاء السيبراني، وتسهيل تبادل الخبرات، والتقنيات.
- تعزيز التعاون بين الدول، وارساء شراكات بين القطاعين العام والخاص، والتنسيق بين مختلف المقاييس الدولية، لتأمين إدارة أكثر فاعلية للمخاطر السيبرانية، وتبادل المعلومات حول الاعتداءات السيبرانية، كما تبادل الخبرات التقنية في مجال الحماية، بما يعزز أمن الأنظمة، والشبكات، وتبادل المعلومات.
- تطوير التعليم ومؤسساته، بادخال برامج تدريس وتدريب متخصصة، بحيث تتأمن عملية نشر الوعي، حول المخاطر السيبرانية، التي تتهدد المجتمع، وجمهور مستخدمي الانترنت، ووسائل حمايتها.
- إلزام المسؤولين عن إدارة الموارد المعلوماتية والاتصالات، في القطاعين العام والخاص، باتخاذ الإجراءات الضرورية للحماية، وبتقييم المخاطر، وبحماية البيانات، والبنية التحتية الخاصة بمؤسساتهم. ويمكن للإجراءات ان تلحظ، تأمين المخاطر، والحوادث التي يمكن ان تقع.

---

[90] وفي أغسطس 2009، أعرب فريق الرصد عن قلقه من إمكانية وقوع حرب سيبرانية تُعطل المجتمع وتُسبب ضرراً لا داعي له ومعاناة لا لزوم لها ولذلك عمد إلى صياغة إعلان إيريتشه لمبادئ الاستقرار السيبراني والسلام السيبراني، الذي اعتمدته الجلسة العامة للاتحاد بمناسبة الدورة الثانية والأربعين للحلقات الدراسية الدولية بشأن الطوارئ الكوكبية في إيريتشه يوم 20 أغسطس 2009. وتم توزيع هذا الإعلان على كل الدول الأعضاء في الأمم المتحدة". الاتحاد الدولي للاتصالات - البحث عن السلام السيبراني *www.itu.int/pub/S-GEN-WFS.01-1-2011*

- لحظ أسس مسؤولية مدنية، تكون قواعدها منسجمة دوليا، وذلك، بموازاة السعي إلى الانسجام، بين القواعد الجزائية. ويمكن لقواعد هذه المسؤولية، ان تبنى على الاهمال، ومخالفة الموجبات الائتمانية، وعدم كفاية تقييم المخاطر، والضرر الذي يلحق بالضحية، نتيجة الجريمة، والاعتداءات السيبرانية.
- أن تعتمد البرامج، والأجهزة الجاهزة، على المصادر المفتوحة، أو أن تكون، على الأقل، مصدقة.
- مناقشة مسائل الأمن السيبراني، في الاجتماعات التي تعقد على المستويات الاقليمية، وليس فقط على المستويات الوطنية، والدولية، بحيث تبرز الخصائص الخاصة بكل منطقة، من خلال خبرائها.
- تعزيز دور المؤسسات الدولية كالانتربول، والاقليمية كالأوروبول، في مجال مكافحة الجريمة السيبرانية.
- مقاربة المسائل العلمية والتقنية، الخاصة بالأمن السيبراني، من جوانبها المختلفة، لاسيما منها، تلك التي تتقاطع مع استخدام التقنيات، مثل الخصوصية، وحماية البيانات، والحريات العامة والخاصة.
- المبادرة إلى مساعدة الدول النامية، والجهات المانحة، على فهم تأثير التقنيات على التنمية، في بيئة تعزز السلامة والأمن، كما تساعد على هدم الهوة الرقمية، بين المجتمعات.

من الملاحظ أن التوصيات، ركزت على مسائل سيبرانية، اتخذت وما زالت، طابع الضرورة والاهمية، مثل الحرب السيبرانية، والإرهاب، والنزاعات السيبرانية بشكل عام، اضافة إلى ضرورة تحقيق التوازن في مجتمع المعلومات، بما يضمن بناء الثقة والاستقرار، من خلال حماية الحريات والخصوصية.

الفصل الرابع
الاعتداءات والجرائم السيبرانية

١ . التميز بين المصطلحين

الاعتداء السيبراني، ذو مدلولات عديدة، تقررها الأهداف، والضحايا، والدوافع، كما الآثار التي يتركها، والنتائج التي يرتبها. فالهجوم على الأنظمة المعلوماتية، يمكن ان يسبب اضرارا محدودة، ويكون نتيجة اهمال دون أي نية جرمية. بينما يمكن ربطه بالأعمال الجرمية، أو الإرهابية، أو الحربية، عندما تكون نتائجه ذات انعكاسات كارثية، على الأفراد، أو المنظمات، أو الدول. لكن قياس نتائج الاعتداءات السيبرانية، يبقى غير ممكن، بدرجة دقيقة.

فمن الصعب على أي كان، الإلمام الوافي، بمدى ونطاق، ارتباط الأنظمة المعلوماتية، واعتمادها على بعضها البعض. كما لا يمكن حصر دراسة النتائج بما يظهر منها، بصورة فورية، لان بعض الاعتداءات، يتم تحضيرها، لإطلاقها بعد أشهر أو سنوات، ولتكون اعتداءات تدريجية، بمعنى استهدافها، لمناطق أو لقطاعات معينة، وعلى مراحل. وبالتالي، لا يمكن قياس الآثار الاجتماعية والاقتصادية للاعتداءات، بما يخدم فهمها بصورة واضحة، واتخاذ الخطوات ألأنجح لردعها، أو الحد من أضرارها.

وغالبا ما يتم استخدام مصطلح «الاعتداء السيبراني»، عوضا عن مصطلح «الجريمة السيبرانية»، للدلالة على اعتداءات موجهة إلى الأجهزة الإلكترونية، والأنظمة المعلوماتية، لاسيما منها تلك المتصلة بإدارة الموارد الحيوية والبنية التحتية، للبلد المستهدف. وغالبا ما تكون الاضرار بهذه البنية والادارات، ذات أثر سلبي، على سمعة البلد ومصداقيته، أو على الاستقرار الاجتماعي، والمالي، والاقتصادي، والعسكري. وتعتبر هذه الأعمال، اعمال عدائية، تتلف الأنظمة، أو توقف عملها، وتتلاعب بالمعلومات. كما يمكن لهذا المصطلح، أن يؤشر إلى عمل عسكري، اذ أصبح من المسلمات، لجوء القوى العسكرية، إلى استخدام التقنيات في عملياتها. أما المؤشر الاهم، الذي يساعد في تمييز «الاعتداء السيبراني»، لاسيما ذاك الذي يمكن تصنيفه، كحرب سيبرانية، عن «الجريمة السيبرانية»، هو النية أو الهدف، كما أسلفنا. وبغض النظر عن حجم المصالح، والمؤسسات المستهدفة بالاعتداء، تبقى النية، العنصر الأهم في التوصيف [91].

وهكذا، يمكن تصنيف بعض «الاعتداءات السيبرانية» نسبة إلى نطاقها، ونتائجها، على الشكل الآتي:

- الاعتداء على الأنظمة التي تتولى إدارة البنية التحتية، كالنقل، وموارد الطاقة، والصحة، والمؤسسات المالية، أو حتى أنظمة المعلومات المعدة لمواجهة حالات التوقف، أو الاعطال، أو اعادة الحال إلى ما كان عليه، باسترجاع مهمات الأنظمة وبياناتها.
- الاعتداء على أنظمة الدفاع، سواء منها تلك المخصصة للهجوم أو للدفاع. وهنا تستبعد قانونية

[91] *When Do We Call a Cyber Attack an Act of Cyber War? - http://blog.trendmicro.com/trendlabs-security-intelligence/when-do-we-call-a-cyber-attack-an-act-of-cyber-war/*

الضربات الاستباقية، في حال الاعتماد على هذا المفهوم، لتبرير الاعتداء.

- الاعتداء على أنظمة الحكومة الإلكترونية، والادارات المختلفة في القطاعين العام والخاص.
- الاعتداء الذي يستهدف التلاعب بالمعلومات، بهدف تضليل السلطات العامة، أو زرع البلبلة في المجتمع، وبين المواطنين.
- التجسس الإلكتروني.
- الرقابة الشاملة، ورصد الاشخاص، وإرهابهم بهدف جمع المعلومات منهم.

في المقابل، يمكن تعريف الجريمة السيبرانية، بالمعنى، الضيق على انها، «جريمة الكومبيوتر» واي تصرف غير قانوني موجه ضد الجهاز، النظام، أو المعلومات التي تحويه، أما بمعناها الواسع، فهي الجريمة المتصلة باستخدام الكومبيوتر؛ اي تصرف غير قانوني، يرتكب باستخدام تقنيات المعلومات والاتصالات ، بما فيه حيازة مواد ممنوعة، أو توزيعها، أو عرضها[92].

ويستخدم مصطلح "الجريمة السيبرانية"، للدلالة على أعمال جرمية محددة قانونا، وعندما يستهدف الاعتداء:

- أمن المعلومات، أي مصداقيتها، وتوافرها، وصحتها. وتندرج في هذا الإطار، عمليات اختراق الأنظمة، عبر سرقة كلمة السر، أو التصيد، أو التضليل والاحتيال، كما عمليات تدمير البيانات، وسرقتها.
- سلامة الاشخاص، كما هو حال التربص والترصد للاطفال، بغية الاعتداء عليهم، واستدراجهم، بهدف استغلالهم جنسيا. كما تندرج هنا عملية استدراج الاشخاص، في إطار عمليات الاتجار بالرقيق، أو تجارة الأعضاء البشرية، أو انتاج المواد الاباحية، أو تقديمها.
- الأموال، من خلال عمليات الغش، والاحتيال، واختطاف الأنظمة، والتزوير، والابتزاز، وتبييض الأموال، الخ....
- المحتوى، كتوزيع مواد اباحية عن الاطفال، أو بث الكراهية، والتمييز العنصري، وعرض خدمات مرتزقة، لتنفيذ عمليات اغتصاب وقتل، والترويج للإرهاب.
- أمن الدولة، وسيادتها، مثل التجسس، وافشاء معلومات سرية.
- الملكية الفكرية، والتي يدخل فيها سرقة البرامج والانتاج الفني، والاستعمال غير الشرعي، لانتاج محمي بالملكية الفكرية.

وكانت اللجنة الأوروبية قد أقرت تعريفا للجريمة السيبرانية، من خلال ثلاثة أنواع من النشاطات الجرمية:

- الجرائم التقليدية (الغش، الخداع، بيع مسروقات، ترويج لممنوعات، التقليد، الاعتداء على الملكية الفكرية، عدم تسليم مبيع بعد قبض الثمن، القرصنة، الخ...)

---

[92] *At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined thus:*
a. *Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.*
b. *Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.*

- جرائم نشر المحتوى غير المشروع، باستخدام تقنيات المعلومات والاتصالات (العنف الجنسي ضد الاطفال، التحريض على الكراهية، التمييز العنصري، التحريض على الانتحار، التعرض للحياة الخاصة، تجنيد ارهابيين، دعارة الاطفال، مواد اباحية تستخدم الاطفال، وصفات المتفجرات، الخ...)
- الجرائم الخاصة بتقنيات المعلومات والاتصالات، اي الاعتداء على الانظمة المعلوماتية (تعطيل عمل الموقع، القرصنة، نشر الفيروسات، الاختراق، الخ...)

ويمكن تمييز هذين المصطلحين، على المستوى القانوني، حيث لا يمكن وصف أي اعتداء ب "الجريمة السيبرانية"، في غياب نص قانوني يوصفها، ويحدد عناصرها، بينما يمكن وصف أي اعتداء ب: "الاعتداء السيبراني"، بمجرد وقوع اي هجوم، وخارج اي نص أو وصف قانوني. فالاعتداء السيبراني، مفهوم واسع يشمل مروحة واسعة من الأعمال، بغض النظر عن التوصيفات، والنصوص القانونية.

لكن، لا بد من الإشارة، إلى نوع من الالتباس، أو الخلط، ناتج عن تداخل الحدود بين "الجريمة السيبرانية"، التي تدخل ضمن إطار اهتمام السلطات المدنية، و"الاعتداء السيبراني"، الذي يمكن ان يندرج في فئة "الحرب الإلكترونية"، والذي يدخل نطاق صلاحيات الأجهزة العسكرية. فالجريمة السيبرانية، كما الحرب السيبرانية، يستخدمان نفس الادوات: البرامج الخبيثة، والفيروسات، واستثمار الثغرات، والدودات الإلكترونية، وغير ذلك من تقنيات رصد، وتسلل، ومنع خدمات. ومنفذو العمليات، ليسوا بالضرورة ممن ينتمون إلى الأجهزة العسكرية، أو الأمنية.

فمع الانترنت المظلم، يمكن للدولة والأجهزة الحكومية، كما للافراد، الحصول على خدمات اي نوع من المرتزقة، وعلى أعلى كفاءات الاختراق، وتوزيع البرامج الخبيثة، وزرع برامج التنصت، وتدمير المعلومات. ومما يثير الالتباس أيضا، أن جمع المعلومات، والتسلل إلى الأنظمة، قاسمان مشتركان بين الاعتداء السيبراني والجريمة السيبرانية. لكن الهدف من وراء عملية الجمع هذه، مختلف، اذ يشكل هذا الجمع في الاعتداء، مرحلة تحضيرية لحرب سيبرانية، بينما يهدف في الجريمة إلى الحصول على الأموال. كذلك، يمكن ان تتشابه الوسائل، والادوات والأساليب المستخدمة للوصول إلى هذه المعلومات، بينما تختلف النتائج.

٢. تصاعد وتيرة التهديدات

وتشير التقارير الموضوعة من الجهات المتخصصة، في مجال مكافحة الاعتداءات على الأنظمة المعلوماتية، إلى تصاعد في وتيرة الاختراقات وسرقة البيانات، والاعداد اليومية للاعمال الجرمية السيبرانية وملايين البرامج الخبيثة، التي تستعمل في ارتكاب الأعمال غير الشرعية، ضد المواقع، والاصول، والأفراد على الانترنت[93].

[93] *http://www.mcafee.com/tw/resources/reports/rp-threats-predictions-2016.pdf*

فقد واكبت الإمكانات التي اتاحها الانخراط في مجتمع المعلومات، فرص مماثلة، للمخالفات والجرائم[94]. وهذا ما دعا العالم بأسره، إلى التنبه والتعاون، في مواجهة ما يمكن أن يعتبر، تهديدا بحجم التهديدات، التي تشكلها الأسلحة النووية، والكيميائية، والبكتيرية[95].

أمام هذا الواقع، نستطيع القول، ان أمن الفضاء السيبيري، يتوقف، بشكل كبير، على الحد من استخدام تكنولوجيا المعلومات والاتصالات، لأهداف جنائية، أو لأغراض تتنافى والمصلحة العامة، لمختلف المجتمعات؛ بعبارة أخرى، على الحد من الجرائم السيبيرانية.

وكانت المقررات الصادرة، عن القمة العالمية لمجتمع المعلومات، قد شددت[96]، على ضرورة بناء الثقة والأمن، في الفضاء السيبيراني. وكانت وثيقة تفعيل خطة عمل جنيف[97]، قد انتهجت الخط نفسه، عندما خصصت الجزء السادس منها، لبناء الثقة والأمن، في استخدام تقنية المعلومات والاتصالات.

٣. اختلاف الدوافع والوسائل

على ضوء الإجراءات الأمنية المتخذة، يحدد المخترق، والمجرم السيبيري، أساليب عمله، وطرق تنفيذه. وعلى أساس مواطن الضعف التي يفترض حمايتها، تحدد المداخل إلى النظام. وعليه، فالمعرفة التي يرصدها ويبحث عنها المجرمون في الفضاء السيبراني، هي تلك التي يملكها المسؤول عن أمن النظام، وعن حمايته. إلا انه، وفي أحيان كثيرة، يملك المجرمون معلومات أكثر تقدما، تجعل اختراق الأنظمة، أكثر سهولة من الدفاع عنها.

ويأتي استغلال نقاط الضعف، أو العيوب الأمنية، في اي نظام معلوماتي، كهدف أول للمعتدين، على أمن الشبكات والانترنت.

وغالبا ما يعمل مقتحم النظام، على خداع المستخدم، عندما يقوم بتزييف صفته، أو انتحال شخصية معينة، ليصل بعد ذلك إلى المعلومات والبيانات، والى كلمات السر. ويساهم في دعم هذه الأعمال غير الشرعية، ما يمكن تسميته بديمقراطية ادوات ووسائل القرصنة، ونشر المعرفة، العائدة اليها، حيث نجد بعض المواقع، التي تتولى توزيع التعليمات، حول نقاط الضعف في الأنظمة المختلفة، والتي يمكن النفاذ منها.

وتختلف نتائج الاعتداء على الشبكات وعلى الانترنت، باختلاف اسبابه، وباختلاف شخصية قائد الهجوم على الأنظمة المعلوماتية. ويمكن تصنيف شخصيات المعتدين، بناء على الأهداف أو الدوافع، حيث نجد الباحث عن التسلية، أو الباحث عن المعرفة، وعن استكشاف كيفية عمل الأنظمة، والخدمات أو الوظائف التي يمكن ان تقدمها. كما نجد من يرغب باثبات قدرته الفكرية والتقنية، أو اثبات وجهة نظر[98]، أو الباحث عن الانتقام وعن وسيلة لإنزال الضرر بالغير، أو بكل بساطة، المجرم الذي يسعى إلى الابتزاز والسرقة، والاعتداء على الأنظمة الاجتماعية والسياسية، واحيانا الدينية.

---

[94] *Crime Fighting Computer Systems and Databases, Sam Vaknin, Ph.D. - 9/10/2005, http://www.buzzle.com editorials/9-18-2005-77050.asp*

[95] *La cybercriminalité est la troisième grande menace pour les grandes puissances, après les armes chimiques, bactériologiques, et nucléaires » - Colin Rose of Buchanan International, a Scottish-basedcompanythatspecialises in tracking down Internet offenders.*

[96] بند 39 ...."نحن نسعى إلى بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات من خلال تعزيز أسس هذه الثقة

[97] صدرت هذه الوثيقة، عن المؤتمر التحضيري رفيع المستوى لقمة تونس، في القاهرة من ٩ إلى ١٠ مايو

[98] *http://www.channel3000.com/technology/2613265/detail.htmlN.C. Man First In Nation Convicted Of Wireless Crime, Man Pleads Guilty To Hacking Into Patient Files.*

كذلك، تتنوع الوسائل والأساليب، اذ يمكن ان تتراوح الطرق المستخدمة بين السلبية؛ والتي تعني مراقبة، ورصد، واعتراض الاتصالات وحركة المعلومات، واستخدام بروتوكولات التعريف بالعناوين وبالاشخاص، وبين الطرق الايجابية؛ عبر اتخاذ المبادرة باللجوء إلى نشر المعلومات، حول كيفية مهاجمة الأنظمة واستغلال نقاط الضعف فيها، وكيفية استخدامها.

٤ . ترتيب الجرائم والاعتداءات بحسب أهدافها

مع تصاعد الاعتماد على الانترنت والاتصالات، تتصاعد مخاطر واحتمالات الجريمة السيبرانية، وتتأكد الحاجة الماسة، الى فهم وتحليل الجرائم، وقراءة خارطة المحيط القانوني لها، لاسيما منها، ذلك الجانب، الذي يتعلق بالأبعاد الدولية. فبالاضافة إلى الأشخاص، تستهدف الجريمة السيبرانية، المنشآت الحيوية والحساسة، مثل المصارف، والمستشفيات، والمحطات النووية، والنقل، والبورصة. وتتوسع مجالاتها، وتمتد، مع التقدم الذي يسجل، على المستوى التقني. فقد سجل العام ٢٠١٥، مثلا، اعتداءات سيبرانية، ارتبطت بأنواع جديدة من التقنيات والأساليب. ويمكن تمييز الاعتداءات والجرائم السيبرانية حسب أهدافها: الأفراد، الأصول والأموال، الدولة. كما يمكن تمييزها بحسب مصادرها، إلى داخلية وخارجية.

أ- الجرائم التي تستهدف الأفراد

يؤدي انتشار الجريمة السيبرانية، إلى خلل عام، قد يهدد المجتمع كله في اقتصاده، وسيادته، وامنه الوطني، كما يمكن لهذه الجرائم ان تهدد النسيج الاجتماعي والأسري، بسبب التشهير، أو إشاعة الأخبار الكاذبة، وسرقة الملفات الخاصة بالأفراد، ونشرها على الانترنت، ووسائل الاتصالات.

تتوزع الجرائم التي تقع ضد الأفراد، بشكل عام، على توزيع محتوى مسيئ، سرقة البيانات، السيطرة على الأجهزة الشخصية، تشويه السمعة، التحرش، الحض على ارتكاب الجريمة، الخداع، سرقة الهوية، انتحال الصفة، الاعتداء على الخصوصية، إفشاء الاسرار المهنية والشخصية، والتصيد والابتزاز. وترتكز هذه الجرائم، بشكل أساسي، على استخدام البيانات ذات الطابع الشخصي، والمحتوى، والأجهزة الشخصية، والاطياف على الشبكات الاجتماعية.

وتسيئ هذه الجرائم، بشكل أساسي، إلى كرامة الانسان، وسلامته الشخصية، عندما تترجم من خلال الاتجار بالبشر، ودعارة الاطفال، والإرهاب على الخط، والتحرش، والملاحقة أو الترصد.

ويعتبر غياب القوانين الرادعة، واتفاقيات التعاون بين البلدان المختلفة، من اهم الاسباب، التي تشجع على هذه الجرائم، اذ ينتقي المجرمون البلدان التي لا إطار قانوني فيها، أو لا تطبيقا فاعلا للقانون، ولا معاهدات تلزمها بمكافحة الجرائم، التي يرتكبونها.

ويسهم انتشار وسائل الاتصال، بالشكل الكثيف الذي نشهده اليوم، في تعريض مستخدمي الانترنت، إلى جميع أنواع المحتوى المسيئ، غير الاخلاقي، وغير المشروع. كما تعرضهم أيضا إلى الالتقاء، بأنواع مختلفة من الاشخاص، الذين يعرضون صداقة كاذبة، تؤدي إلى الايقاع بالبعض منهم، في متاعب

خطيرة، أحيانا كثيرة، كما تتيح فرص الاعتداء عليهم. ويعود السبب في ذلك، إلى الشعور بالامان، أو البحث عنه على الشبكة العالمية للمعلومات، أو إلى خطأ في تقدير نتائج وعواقب نشر بعض البيانات ذات الطابع الشخصي، والافشاء ببعض الاسرار. وتبرز في هذا الإطار، بشكل خاص، الاعتداءات التي تقع على الاطفال، والأخطار التي يتعرض لها الشباب.

وتزيد المجهولية، كما امكانات اخفاء الهوية الحقيقية، وانتحال هوية مزيفة، من خطورة الموضوع، اذ انها تسمح للمعتدي، بارتكاب ما لا يجرؤ على ارتكابه، في العالم المادي، كتوجيه الاتهامات، وإرهاب الآخرين، والتنمر. ويزيد في ارتفاع حظوظ التعرض للاعتداءات، الانتشار الواسع للتطبيقات المعلوماتية، التي تسمح بالاتصال المباشر، بين شخص وآخر، كبرامج المراسلات المباشرة، مثل الواتساب والفايبر والمسينجر، أو بعدد من الاشخاص، كالمدونات، وغرف الدردشة، ووسائل التواصل الاجتماعي، التي ساعدت في تنمية واظهار الميل إلى الاستعراض، لدى الشباب بشكل خاص، ولدى شريحة كبرى من المجتمع، بشكل عام.

كذلك يسمح اخفاء الهوية، الذي تتيحه التقنيات للمترصدين والمجرمين، باستدراج مستخدمي الانترنت، إلى الافصاح عن بياناتهم الشخصية، أو عن صورهم الحميمة، أو إلى ارسال الأموال إليهم، باللعب على العامل النفسي لدى الشخص الآخر، لاشعاره بالامان والحميمية، أو بالرغبة في المساعدة، أو حتى بالخوف، نتيجة تهديدات معينة، بكشف أسرار أو معلومات شخصية. وغالبا ما يقوم المترصد، أو المطارد، بجمع المعلومات الشخصية عن الضحية، مثل اسمه، معلومات عن عائلته، أرقام هواتفه، مكان الاقامة، ومكان العمل، وما إلى ذلك، عن طريق مواقع الشبكات الاجتماعية، والمدونات، وغرف المحادثة، وغيرها من المواقع.

ـ استغلال الاطفال والقاصرين في مواد إباحية

ويشير هذا المصطلح، إلى ظهور الأطفال والقصر (الذين تقل أعمارهم عن ١٨ عاما)، في صور أو أفلام، أو مشاهد ذات طبيعة وايحاءات إباحية، أو مضمون جنسي، بما فيها مشاهد أو صور للاعتداء الجنسي على الأطفال، وهي جريمة يعاقب عليها قانونيا، في أغلب دول العالم. كما وتتعامل أغلب دول العالم، بحزم وجدية، مع هذا النوع من الجرائم، مع كل من تثبت عليه تهمة الاحتفاظ، أو الاتجار، أو تداول صور أو أفلام إباحية، وتحذو حذوها المنظمات الدولية، مثل اليونسيف، والشرطة الدولية «الإنتربول».

كما يلجأ بعض المترصدين، إلى دعوة الضحية إلى اللقاء بهم، وجها لوجه، احيانا كثيرة، لاسيما منهم، المترصدون بالاطفال، وأصحاب الميول الجنسية غير السوية، والسوابق الجرمية. وقد بينت عدد من الحالات التي سجلت، حصول اعتداءات جنسية، وجرائم قتل، أو اختفاء الاشخاص، نتيجة هكذا لقاءات. فمن الصعوبة بمكان، ثني الاطفال والشباب عن التواجد على الانترنت، وعلى وسائل التواصل الاجتماعي. ويزيد في خطورة الامر، ما تشعرهم به هذه الوسائل من امان، عندما تصور لهم انهم في بيئة صديقة وآمنة. وهذا ما يفسر سهولة استدراج الاطفال والمراهقين، إلى تبادل مواد جنسية، تحرجهم لاحقا، وتجعلهم ضحية أكيدة، لمروجي دعارة الاطفال، والخاطفين، والمتاجرين بالبشر.

ويلاحق الخطر البالغين أيضا، اذ تسمح الانترنت، بتكوين مجموعات حول اهتمامات مشتركة، يمكن ان تكون غير شرعية، ليس اقلها، المواد الاباحية، والمواد التي تعرض عمليات قتل، أو مواد غير اخلاقية اخرى.

من الناحية القانونية، تمنع العديد من البلدان العربية، تداول المواد الاباحية، كما يلجأ بعضها، إلى حجب المواقع التي توزعها، وكذلك يجرم العديد منها، المواد الاباحية الخاصة بالاطفال، أو مواد الاعتداء عليهم.

لكن المجتمع العربي، لا يبدو بعيدا عن هذا الحظر، بالرغم من حرص الدول على حماية مجتمعاتها ضد المحتويات المسيئة، اذ سجل احد التقارير الذي اصدره محرك البحث غوغل، احتلال عمليات البحث عن المواد الاباحية، في البلدان العربية، تقدما ملحوظا، على بقية دول العالم[99].

على خط مواز، تزدهر الأعمال الجرمية، التي تجمع بين مكونين أساسيين، هما الجنس والمال. ويمكن ملاحظة هذا الامر بشكل واضح، من خلال انتشار المواقع، التي تعلن عن تأمينها الشريك المناسب، أو الشخص الثري، أو بكل بساطة، الربح السريع والسهل، بينما يختفي وراءها، أحيانا كثيرة، مترصدون يبحثون عن شركاء في تبييض الأموال، أو الاتجار بالرقيق، أو توزيع المواد الاباحية. وتشارك هذه المواقع، في تعزيز تطور صناعة المحتوى غير المشروع، وانتشار الاعتداءات على الاشخاص. أما المثال الاوضح على ذلك، فهو موقع Craiglist، الذي يروج لبيع السيارات وبضائع اخرى، ويستضيف، كما يروج، لمواقع ومواد اباحية، أدت إلى عمليات استغلال للاطفال، في تصوير مواد اباحية، وفي بيعهم، بهدف عمليات دعارة[100].

وتستخدم الانترنت أيضا، سواء عبر الرسائل القصيرة، أو مجموعات النقاش، أو وسائل التواصل الاجتماعي، في دعم السلوك العدائي، من قبل مجموعة، أو من قبل فرد واحد، بهدف ايذاء الآخرين، فيما يعرف بالتنمر السيبراني. ويأتي في هذا الإطار، القمع، وتشويه السمعة، عبر نشر افتراءات، أو صور ومعلومات، صحيحة حتى. ويمارس التنمر على الاطفال، كما على البالغين. ويشابه التنمر فعل جرمي آخر، هو الترصد السيبراني، أو المطاردة السيبرانية، في المنتديات العامة، وغرف الدردشة، أو على مواقع التواصل الاجتماعي. ويسعى معظم المترصدين، إلى تأليب الآخرين على الضحية، وتشويه سمعتها، والحط من قدرها، في نظر محيطها. وغالبا ما تتضمن عملية المطاردة، تهديدا وسرقة هوية، وسرقة معلومات، وخطابات كراهية، وطلب ممارسات غير اخلاقية، منها الجنس. ويعتبر تكرار عمليات الرصد والمتابعة، تحرشا سيبرانيا، يؤشر إلى اضطرابات، في شخصية المتحرش [101].

[99] *Pakistan tops list of most porn-searching countries: Google. http://tribune.com.pk/story/823696/pakistan-tops-list-of-most-porn-searching-countries-google/*

[100] *Craigslist's shame: Child sex ads- By MalikaSaada Saar, Special to CNN " Last month, two girls trafficked for sex through the website Craigslist wrote an open letter to its founder, Craig Newmark, pleading with him to get rid of the adult services section, where sex ads are placed." http://edition.cnn.com/2010/OPINION/08/02/saar.craigslist.child.trafficking/*

[101] *www.cyberbullying.ca/pdf/Cyberbullying_Article_by_Bill_Belsey.pdf. Cyberbullying: An Emerging Threat to the "Always On" Generation By Bill Belsey, President and Founder of Bullying.org*

ب- الجرائم الواقعة على الأصول والممتلكات

تتخذ هذه الجرائم الملكية هدفا لها، وتطال الجهات الحكومية، والخاصة، والفردية، دون استثناء، اذ انها تركز على تدمير الملفات واتلافها، وعلى البرامج الخاضعة لحقوق الملكية الفكرية والصناعية، وذلك عبر برامج ضارة، يتم نقلها إلى الأجهزة، بطرق مختلفة، منها البريد الإلكتروني.

وتزدهر هذه الأعمال، كامتداد للاعمال الجرمية، في الواقع المادي، وكوسيلة للوصول إلى العنصر الأهم في المؤسسات التجارية أو الحكومية على الانترنت، الا وهو البيانات والمعلومات.

وقد سمحت الانترنت، باستنباط وسائل جديدة لجمع الأموال، والتقليل من احتمالات كشف المجرمين، عبر استخدام تقنيات الاتصال والمعلومات. ويمكن ارتكاب هذه الجرائم، من قبل فرد واحد، من وراء شاشة جهازه، أو من قبل مجموعات صغيرة، أو عصابات منظمة.

كما تؤمن العديد من المواقع، الخبرات والبرامج اللازمة، لعمليات الاختراق، ومحو الآثار، والتصيد، مما يسهل ارتكاب الجرائم السيبرانية. كما تساهم الانترنت، في تسهيل عملية تبادل المعلومات، وتنظيم الجهود، بين مختلف المجرمين السيبرانيين، مما يعطي الجريمة السيبرانية دفعا اقوى، ويعزز فرص نجاحها.

وبالفعل، فقد تأثرت الجرائم الاقتصادية ايجابا، بقدرات تقنيات المعلومات والاتصالات، التي تحولت إلى جزء أساسي من وسائل ارتكاب الجرم، وحيث يفيد المعتدون من السرعة في التنفيذ، والمجهولية، وامكانية اخفاء الاثر، والقدرة على تجاوز الحدود الجغرافية، دون خطر.

وتتمحور الاعتداءات في هذا الإطار، على استغلال وجود المؤسسات المختلفة على الانترنت، واتصال النشاطات المالية بالشبكة، حيث تستعمل أنظمة الدفع الإلكتروني، والنحويل، والتجارة، ليس فقط عبر التسلل إلى الأنظمة، وانما أيضا من خلال استخدام بيانات شخصية، للافراد المسؤولين عن إدارة الأموال، وتحويلها إلى حساباتهم الشخصية، أو إلى حسابات اخرى، توزع فيما بعد عليهم. ولعل أدهى المخاطر، التي يمكن ان تواجه الاقتصاد الرقمي، هي تلك التي تواجه الاقتصاد التقليدي، ونعني بها تبييض الأموال.

ج- التصيد

ومن الأساليب التي تشكل استخداما مضرا، لتكنولوجيا المعلومات والاتصالات، وتهديدا لأمن الانترنت، الphishing أو التصيد، حيث يمكن توريط مستخدم الانترنت، في فضح معلومات سرية، أو في ارتكاب جرائم كتبييض الأموال، والتعدي على الملكية الفكرية، وتسهيل أعمال ابتزاز، عندما تكون المعلومات المكشوفة، أسرارا صناعية، أو مالية، أو تجارية.

وتتم عمليات التصيد، من خلال البريد الإلكتروني، حيث يتم توجيه رسائل، يطلب فيها من المرسل اليه، اعطاء رقم حساب مصرفي، ليتم تحويل مبالغ معينة اليه، مقابل نسبة مئوية من المال. أو يمكن أن يطلب اليه، تيويم معلومات حسابه المصرفي، وتعديل كلمة المرور أو تأكيدها، أو تعديل أو تأكيد، أي معلومة، أو بيان شخصي آخر، يمكن أن يساعد منفذي عمليات التصيد، في استخدام هوية الشخص المستهدف، للدخول إلى نظام مالي، أو اقتصادي، أو اجتماعي، يعمل عليه. ولا تنحصر المحاولات

في البريد الإلكتروني، بل تتعداه إلى التراسل المباشر، حيث يلجأ القراصنة، إلى توجيه رسائل تقود إلى وصلات، يكفي الضغط عليها، لتحميل برامج تجسس، أو فيروسات على الجهاز، الذي يتم عبره الاتصال[102].

ففي عملية اقتحام لنظام احدى الشركات التي تقدم خدمات تحويل أموال، في الولايات المتحدة الأميركية، تمكن المجرمون، من الوصول إلى أسماء أصحاب ملايين بطاقات الائتمان، وأرقامها، ورموز الامان فيها[103]. وقد اكتشف هذا الأمر، على أثر تحديد وجود بعض التحويلات غير الشرعية fraudulent، من قبل نظام الامان الخاص بتعقب التحويلات لدى ماستر كارد، ما دفع الشركة إلى طلب مساعدة أحد المصرفيين، الذي تمكن من تحديد وجود المشكلة، لدى الشركة التي تتولى عمليات التحويل.

كما تم بمناسبة هذه العملية، الكشف عن مخالفة هذه الاخيرة، لسياسة الامان المعتمدة لدى ماستر كارد، والتي تمنع على الشركة التي تتولى التحويل، أن تحتفظ بمعلومات عن بطاقات الائتمان. وكانت شركة كاردسيستمز، قد احتفظت بمعلومات، عن جميع التحويلات التي لا تتم الموافقة عليها.

وفي قضية اقتحام أخرى، تعرضت جامعة أوهايو، لعملية قرصنة على البيانات الخاصة، لمدة سنة كاملة، من قبل مقتحمين Hackers، في الولايات المتحدة الأميركية وخارجها، وطالت العملية، فيما طالت، أرقام الضمان الاجتماعي، لـ١٣٧ ألف شخص[104].

فبالاضافة إلى الشركات، والمؤسسات المالية، تعتبر الجامعات والمدارس، في الدول المتقدمة تقنيا، مصدرا هاما للبيانات والمعلومات الشخصية، التي يستهدفها القراصنة. ذلك أن الأنظمة المعتمدة في هذه المؤسسات، تركز، بشكل أساسي، على تسهيل الوصول إلى المعلومات، من جهة أولى، كما تفتقر إلى أساليب الحماية والأمن الفاعلة، من جهة ثانية.

أمام هذا الواقع، تبدو الحماية الذاتية، من قبل الأفراد والمؤسسات، كما اللجوء إلى بعض التقنيات، كتقنية التشفير، خطوة احترازية لا بد منها، للمساهمة في تحقيق الأمن على الانترنت. الا أن الطبيعة التقنية العالية، التي تتميز بها الانترنت، تجعل هذه الخطوة، غير أكيدة النتائج في كل الاحوال، ما يستدعي حتمية وجود القانون، وضرورة قيام الدولة، بدورها التقليدي في الرقابة، كخطوة نحو تدارك حدوث الفعل الضار، ومنعه.

د- الجرائم التي تستهدف الدولة

إذا أخذنا طبيعة المخاطر، التي يمكن ان تطاول المجتمع التقليدي، والمجتمع السيبيراني، على السواء، نجد انهالا تنال فقط من الحقوق والحريات الشخصية، الاجتماعية والتجارية والعلمية، وإنما أيضا، من مصالح الدول وأمنها، واستقرار مؤسساتها وأنظمتها، والنسيج الاجتماعي فيها.

---

[102] *Heartworm infects Microsoft›s IM network Instant-messaging system in need of a vet, September 26, 2006, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9003623&source=rss_news50*
[103] *CNNMoney.com, 40M credit cards hacked. Breach at third party payment processor affects 22 million Visa cards and 14 million MasterCards. July 27,2005, by Jeanne Sahadi.*
[104] *www.News.com.CNET.*

ففي عصر المعلومات، لا يمكن لأية حكومة، أو إدارة، سواء في العالم الثالث، أم في الدول الأكثر تقدما، أن تنأى بنفسها، عن الهم الذي يمثله اختراق الشبكات، والتعرض لأمنها.

وبالتالي، فان المعنيين بتأمين الأمن في مجتمع المعلومات، هم جميع العاملين، سواء انتموا إلى القطاع العام، ام إلى القطاع الخاص. ونعني بذلك، الحكومات؛ وما تمثله من ادارات رسمية، والقطاع الخاص، والمجتمع المدني. الا ان الدور الأبرز، يبقى دور التقنيين، في كل من هذه القطاعات. لان الانكشاف التقني، بمعنى غياب الثقة في قدرة المواصفات الفنية للشبكة، وللبرامج، على تامين الحماية والامان، لما ينتقل عليها، أو لما يمكن ان يتم عليها من معاملات، يعني غياب الثقة في مجتمع المعلومات، وفيما يمثله من قدرة، على تحقيق التطور والنمو.

وإذا كنا نميل، وعلى غرار ما تميل اليه جميع الحكومات المتقدمة، والمنظمات الاقليمية والدولية، إلى اعتبار الأمن القانوني، خطوة أساسية على طريق تسخير تكنولوجيا المعلومات والاتصالات في خدمة النمو والتنمية، فاننا نرى أيضا، ان القانون، قادر على حسم معركة الحماية على الانترنت، لاسيما مع إقرار الخبراء والمختصين، بان الأمن التقني على الانترنت، صعب التحقيق.

فالتقنية ليست العامل الذي يمكن الركون اليه، بشكل أكيد وحازم، في تحقيق الأمن. وقد اثبتت الوقائع، انه لا بد من وازع ومن رادع، يواكب هذا العامل، ويعطيه بعدا أكثر فعالية. لكن ذلك، لم يمنع العديد من الحكومات، من الاتجاه نحو البحث عن الحماية، في كنف التقنية، حيث تم إقرار برامج حماية، وخطط تطوير لانظمة دفاع، ضد الاعتداءات الآتية من الفضاء السيبيري. فقد انتقل الاهتمام الذي كان مخصصا للتطويرات العسكرية التقليدية، إلى الاهتمام بإيجاد الوسائل الملائمة لطبيعة الخطر السيبيري، والكفيلة بتداركه وردعه.

فالخطر على الانترنت، برأي كبار المسؤولين، لا يقل شأنا وتأثيرا، عن الاعتداءات والهجمات، التي يمكن ان تحصل في العالم المادي[105]. وكان وزير الداخلية في الولايات المتحدة الأميركية، ميشال شرتوف، قد أكد، ان بلاده تعمل على تطوير نظام دفاع، يمكنه صد الاعتداءات على الشبكات وعلى الانترنت. ويهدف المشروع، فيما يهدف، إلى الحد من نقاط الاختراق على الشبكات، لاسيما منها، تلك الخاصة بالأجهزة الحكومية.

في سياق ما تقدم، تركز الاطراف المعنية جهودها، على عدد من المحاور، التي تتكامل فيما بينها لتحقيق الأمن، كالإطار التشريعي، والتعاون الدولي، وبناء القدرات والبنية التنظيمية، والتدابير التقنية.

ويمكن تصنيف الاعتداءات، التي تستهدف المؤسسات الحكومية والدولة، بشكل عام، تحت عدد من أنواع الجرائم، نذكر منها:

- التلاعب بالمعلومات
- حرب المعلومات
- التسلل إلى أنظمة البيانات الحكومية، واختراق الأجهزة الحكومية، التي تدير البنية التحتية والبنية الحرجة

[105] *www.csooline.com/article Robert McMillian, IDG News service (San Francisco Bureau), RSA: DHS Project will secure fed's computers. Homeland security secretary Michael Chertoff said he takes cyber threats as serious as threats in the physical world.*

- الرقابة والتجسس
- الحرب السيبرانية
- الإرهاب الإلكتروني، أو الإرهاب الجماعي
- تسريب المعلومات واختطافها
- الاختراق النضالي
- التجسس الإلكتروني

ونتوقف في هذا السياق، عند أعمال التجسس، لاسيما على المستوى الاقتصادي، والسياسي، والذي يمكن ان تتعرض له أجهزة الدولة كافة، ومؤسساتها، كما يتعرض له الأفراد، ومؤسساتهم. ففي كلمة القاها الرئيس بيل كلينتون، في العام ١٩٩٤ في الCIA[106]، بدا واضحا الاتجاه، نحو إقرار دور جديد للمخابرات، في مجال مراقبة الاتصالات والمعاملات الإلكترونية. وكان الرئيس الأميركي، قد أكد على دور المخابرات الأميركية، على مستوى المساهمة في رخاء ورفاهية الولايات المتحدة الأميركية، مع ما يعنيه ذلك، من دور على المستوى الاقتصادي، لا بد وان يتبلور في أحد اشكاله، برصد وملاحقة المعلومات الاقتصادية، الخاصة بالبلدان الصديقة والعدوة. لا بل ان التنصت والرصد والملاحقة، يمكن ان تطاول المواطنين العاديين، والمؤسسات الوطنية، بما يتعارض مع مبادئ الحفاظ على الحريات، وعلى الحق في الخصوصية. وكانت وسائل الإعلام الأوروبية، اضافة إلى المسؤولين، قد نددت بتسخير تكنولوجيا المعلومات والاتصالات، من قبل الولايات المتحدة الأميركية، لاغراض التجسس، لاسيما الصناعي والاقتصادي منه[107].

فبعد انتهاء الحرب الباردة، كان لا بد للعديد من اجهزة المخابرات حول العالم، لاسيما منها الأميركية والأوروبية، ان تجد الدوافع، التي تدعم استمرار حصولها على موازنات مرتفعة القيمة، وتحافظ على دورها وسيطرتها. وفي هذا الإطار، اعيدت عملية تحديد مفهوم الأمن الوطني، بحيث شملت الاقتصاد، والتجارة، والعديد من نشاطات الاتحادات المختلفة.

ولعل اهم ما يمكن ذكره في هذا المجال، هو نظام التنصت الأميركي، الذي يمكن القيمين عليه، من التنسيق بين المعطيات، التي تبث بواسطة اثني عشر قمراً اصطناعياً.

ويعتبر هذا النظام، من اقوى انظمة التجسس، حيث يتألف من شبكة واسعة من محطات التجسس الإلكترونية، المنتشرة حول العالم، والتي تديرها خمس دول، هي الولايات المتحدة الأميركية، وانكلترا، وكندا، واستراليا ونيوزيلندا، والتي ترتبط فيما بينها بواسطة اتفاق سري.[108]

---

[106] *newsmax.com Staff for the story behind the story…Clinton used NSA for economic Espionage. Monday, Dec, 19, 2005. http://archive.newsmax.com/archives/ic/2005/12/19/114807.shtml.*

[107] *"and the NSA, as the biggest and wealthiest communications interception agency in the world, is best placed to trawl electronic communications and use what comes up for US commercial advantage" newsmax.com Staff for the story behind the story…Clinton used NSA for economic Espionage. Monday, Dec, 19, 2005. http://archive.newsmax.com/archives/ic/2005/12/19/114807.shtml.*

[108] *Patrick S. Poole. "ECHELON: America's secret Global surveillance Network". http://fly.hiwaay.net/~pspoole/echelon.html ECHELON is actually a vast network of electronic spy stations located around the world and maintained by five countries: the US, England, Canada, Australia, and New Zealand. These countries, bound together in a ءstill-secret agreement called UKUSA, spy on.*

وكانت احدى الصحف السعودية قد نشرت مؤخرا[109]، خبر تعرض عدد من الجهات الحكومية ، لمحاولات اعتداء، عن طريق رسائل بريد إلكترونية، اصطيادية (Phishing email)، مرفقة بملفات تتولى زرع البرامج الخبيثة على الجهاز، فور فتحها، كما تتولى سرقة المعلومات، منه، واعادة ارسال نفسها، بطريقة أوتوماتيكية، إلى حسابات بريد إلكتروني آخر، لتنفيذ العمليات نفسها.

وأكد مسؤول عن الأمن الإلكتروني، في المملكة العربية السعودية، بعد اعتداءات على انظمة حكومية، في العام ٢٠١٥، انه قد سجلت اعتداءات عديدة، في السابق، استهدفت بعض الشخصيات السعودية، وعدد من البلدان العربية، من قبل ميليشيا إيرانية تدعى «روكت كيتن»، تعتمد على إنشاء حسابات مزيفة، وأسماء وهمية أو مستعارة، وإرسال بريد إلكتروني مع مرفق. وقد أشار أيضا، إلى ان هدف هذه الميليشيا السيبرانية، كما أصبح معلوما، هو التجسس على عدد كبير من الشخصيات، تمكنت بنتيجته من جمع معلومات، عما يقارب ال ١٦٠٠ من الأهداف البارزة، حول العالم.

٥. المحتوى غير المشروع

بالرغم من الارتباط الوثيق، بين نشر المحتوى غير المشروع والجرائم الإلكترونية، فاننا نرى ضرورة ابرازه، كنقطة مستقلة. فانطلاقا من مقولة ان ما هو غير مشروع على المستوى التقليدي، يبقى غير مشروع في الفضاء السيبيراني، لا بد من النظر إلى المحتوى غير المشروع، كاحد المخاطر التي ترتبط مباشرة بأمن المجتمع والدولة، على السواء، ما جعل تنظيم وتشريع ما يمكن تداوله من معلومات، بواسطة اي من وسائل النشر، مسألة لصيقة بمهمات الدولة الأساسية في حماية المجتمع، وحماية النظام القائم فيه. وبما ان مهمات الدولة لم تتغير، يبقى المحتوى غير المشروع، على الشبكة العالمية للمعلومات، وعلى وسائل النشر الإلكترونية كافة، في طليعة المسائل، التي لا بد من تأطيرها وتنظيمها. والمحتوى غير المشروع، يدعو إلى التوقف عنده، على أكثر من مستوى، ونكتفي هنا، بالمستوى الإعلامي، ومستوى حماية الأطفال والشباب والثقافة التي ترتبط بهما. فممارسة النشر والإعلام الإلكتروني، سواء عبر المواقع الإعلامية الرسمية، أو عبر المدونات، والصفحات الشخصية على المواقع الاجتماعية، حولت مواقع عديدة، على الشبكة العالمية للمعلومات، إلى منابر إعلامية، تطرح وتناقش، مختلف الآراء، والتوجهات والسياسات.

على خط متصل، يطرح بث بعض أنواع المعلومات، والصور، والخدمات على الانترنت، إشكالية حماية الشباب، والأطفال بشكل خاص، من المحتوى غير المشروع. ونذكر على سبيل المثال: عرض خدمات الدعارة، وبيع الكحول، والمواد الطبية غير المشروعة، والاستشارات الطبية غير المشروعة، والفلك، والميسر، والخطابات العنصرية، والمواقع الخاصة ببدع ومعتقدات، تحرض على الانتحار أو على قتل الآخرين، هذا عدا عن المواد الاباحية التي تستخدم الأطفال، وتستغلهم.

وإذا اضفنا إلى كل ما تقدم، غياب تعريف عالمي، أو حتى إقليمي، لما يمكن اعتباره محتوى غير مشروع، بحسب ما تفرضه فعالية المكافحة، في الفضاء السيبراني، ندرك خطر هذا النقص، وانعكاساته العملية.

[109] *http://www.okaz.com.sa/new/Issues/20160517/Con20160517839900.htm*

وعليه، لا بد من العمل، للوصول إلى إيجاد أرضية مشتركة، ومبادئ عمل، تمكن من مكافحة المحتوى غير المشروع. وهنا يمكن للتقنيات، أن تلعب دورا أساسيا، لاسيما من خلال تطوير برامج الترشيح والفلترة، بناء على تعليمات محددة لهذا المحتوى غير المشروع، بحيث يمنع وصوله، على الأقل إلى الاوطان التي تعتبره كذلك. وهنا أيضا، تبدو الحاجة ملحة، لمعالجة المدلول الواسع والمطاط، للمحتوى غير المشروع، في بعض التشريعات الوطنية، والتي يمكن معها للسلطة، أن تتصرف بالتفسير والقياس، إلى درجة عالية، ما يؤشر إلى امكانات واسعة للاعتداء على حرية التعبير، وغيرها من الحريات المرتبطة بها، كالحق في الخصوصية، والحق في التعبير عن الرأي.

٦. التقنيات في الحماية

يعتبر إنشاء حماية على الجهاز المضيف، من أكثر الطرق فاعلية، واقلها كلفة، في تأمين حماية الأجهزة المتصلة على الشبكة. وغالبا ما يلجأ في هذا المجال إلى ما يعرف بجدار النار Firewall[110]، وبرامج التنقية[111]. وتعتبر هذه البرمجيات، من الادوات التي تستخدم في حماية الأنظمة، كما في منع الوصول إلى مواقع، أو معلومات معينة. فالتنقية من الادوات التي تستعمل لحماية بعض الفئات الاجتماعية والعمرية (الاطفال والشباب)، الا انها تلعب دورا في الحماية، عندما تمنع الدخول إلى مواقع يمكن ان تحتوي برامج، وفيروسات، وغيرها من البرمجيات الضارة.

ويعتمد في حماية البيانات أثناء عبورها، عدد من البروتوكالات، كنظام أمن الاتصالات(SSL)، أو الISPEC. وتستخدم بروتوكولات الحماية، تقنيات، تدعم الترميز والتشفير. في هذا الإطار، يجب الانتباه، إلى ان الترميز والتشفير، ليسا سوى جزء من الحماية، التي يجب أن تطاول، ليس فقط المعلومات، وإنما البرنامج أيضا. كما يفترض الانتباه هنا، إلى المكان الذي يحفظ فيه، مفتاح فك الشفرة والرمز. ومن الافضل، التعامل في هذا المجال، مع الحل الأمني، الذي تواكبه عملية تصديق جهة ثالثة[112].

أ– التشفير

يعتبر التشفيرcryptography[113]، من التقنيات التي يمكن اللجوء اليها، كوسيلة أساسية في حماية المعلومات الشخصية، والمعلومات السرية. فالتشفير، تقنية تساعد على حماية المعلومات، عبر تحويل النصوص إلى رموز لا يمكن قراءتها، الا بعد اعادة تحويلها إلى نصوص مقروءة، من خلال عملية تفكيك هذه الرموز Decryption.

[110] *A firewall is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system. It is also a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria.http://en.wikipedia.org/wiki/Firewall*

[111] *Internet filter,» refers to a form of computer software sold commercially, designed to be installed on computer terminals providing access to the Internet, which operates to prevent access to information by filtering out certain information otherwise available on the Internet. http://www.hudsonville.org/Library/internetpolicy.html*

[112] *Example: Data Encryption has been certified by the federal Information Processing Standards (FIPS) which is a universally respected governmental certification agency.*

[113] *Cryptology is the science of coding and decoding secret messages. (Crypto is the Greek root for secret or hidden). It is usually divided into Cryptography, which concerns designing cryptosystems for coding and decoding messages, and the more glamorous Cryptanalysis, which is concerned with ``breaking" cryptosystems, or deciphering messages without prior detailed knowledge of the cryptosystem. David J. Wrigh,t 1999-11-19*

ـ أنواعه

وتستخدم في العمليتين، مفاتيح سرية خاصة[114]. ومن تقنيات التشفير الكلاسيكية المعتمدة على الشبكات، نوعان أساسيان، هما: تقنيات التشفير المتناسق Symmetric أو ال Secret Key، وتقنيات التشفير غير المتناسقAsymmetric. تقوم التقنية الأولى، على استخدام مفتاح واحد متشابه، بين مرسل البيانات أو المعلومات ومتلقيها، بينما تقوم الثانية، على وجود مفتاح عام واحد، وعلى استخدام مفتاحين مختلفين، من قبل كل من المرسل، والمرسل اليه.

فمقابل تقنية التشفيرCryptography، تقنية فك الشيفرة Cryptanalysis.واذا كانت الأولى، معنية بتأمين حاجز للمحافظة على أمن المعلومات، والبيانات وصحتها، ومصداقيتها، فان الثانية، معنية بإسقاط هذا الحاجز، وتفكيكه، لكشف المعلومات، واقتحام أسرار الأفراد، والشركات، والدول. ومن أنظمة التشفير الأكثر انتشارا، وفعالية، في حفظ سرية المعلومات، التي تنتقل عبر الانترنت، تقنية ال DES، والتي تعتمد على تشفير أصغر أجزاء الرسالة، أي البيت BIT. ويسجل لهذه التقنية، صعوبة كسر الشفرة، لاسيما وأنها تؤدي إلى تغيير محتوى الرسالة، لدى أي خطأ يرتكب على مستوى فكها. وإذا كانت طريقة عمل تقنية الDES، معروفة ومنتشرة، فان المفتاح المستخدم للتشفير، ولفكه، يبقى غير معلوم.

كذلك ينتشر استخدام تقنية تشفير تعرف بالPGP [115]، التي طورها فيليب زيمرمان، وهي عبارة عن مجموعة برامج، طورت بالاعتماد على بعض أنظمة التشفير، والبروتوكولات المميزة المرتبطة بالبريد الإلكتروني، وتتميز بامكانية العمل مع أنظمة تشغيل متعددة. وأنظمة التشفير المستخدمة في هذا النوع من البرامج، هي ذاتها المحددة في تقنية RFC ٢٤٤٠، وتستخدم فيها أنظمة مختلفة في عملية نقل المفتاح، وفي تشفير الرسائل، وفي التوقيع الإلكتروني.

ولتقنية التشفير دور هام، في الحماية من عدد من الجرائم السيبرانية، لاسيما وانها تحمي المعلومات، والبيانات الشخصية؛ كتلك المتعلقة ببطاقات الائتمان، والأسماء والعناوين، ومضمون الرسائل الإلكترونية، والمعلومات التي تنقل عبر شبكة الانترنت، وذلك في حال اعتراضها، أو الوصول اليها، دون رغبة صاحبها. كذلك، تستخدم تقنيات التشفير، في مجال تأكيد مصداقية الوثائق الإلكترونية، وضمان صحة المعلومات والبيانات، لاسيما منها التوقيع، مايمنع التلاعب بمصداقية الوثائق والمعلومات.

ويعتمد على التشفير أيضا، في العديد من برامج وأنظمة الدفع والايفاء، على الانترنت، التي تستخدم العملة الرقمية، ومعالجة الشيكات، والتحويل الإلكتروني للأموال، وما إلى ذلك.

[114] *Cryptology refers to the twin processes of «encryption» - the conversion of ordinary information («plaintext») into a superficially unintelligible code («ciphertext») - and «decryption» - the conversion of ciphertext back into plaintext. Encryption and decryption are performed using a set of mathematical algorithms of varying complexity, known collectively as a «cipher». A «key», in turn, controls access to the cipher. In other words, without the key, you can›t break the cipher.Thales, expert in cryptology. http://www.thalesonline.com/uk/Press-Room.html*

[115] *Pretty Good Privacy*

ـ خطوات داعمة

لكل ما تقدم، تتجه غالبية الدول المتقدمة، في مجال استخدام تكنولوجيا المعلومات والاتصالات، سواء في الاتحاد الأوروبي، أو في أميركا، إلى دعم استخدام هذه التقنية، بعد أن كانت قد حاولت السيطرة عليها، عبر وضع حدود خاصة باستعمالها، واستيرادها أو بتصديرها. وكانت ال OECD[116]، قد وضعت خطوات توجيهية، خاصة بسياسة التشفير، استند إليها العديد من البلدان، في وضع سياسته الوطنية في هذا المجال، ومنها كندا وألمانيا، وايرلندا وفنلندا. كما صدر تقرير عن اللجنة الأوروبية في العام ١٩٩٨[117]، شدد على ضرورة دعم استخدام هذه التقنية، ورفع الحظر عن المنتجات والخدمات، التي تهدف إلى تطويرها، ونشر استخدامها.

في هذا الإطار، تساهم العديد من الحكومات، ومؤسسات القطاع الخاص، وبعض المنظمات، الاقليمية والدولية، في تطوير مجموعة المعايير الخاصة بتقنية التشفير، ومن تلك المنظمات: ال ISOو ANSI وIEEE وNIST وIETF. وتتنوع هذه المعايير، بتنوع المجالات التي تطبق فيها، كتلك التي تطبق في القطاع المصرفي، أو تلك الخاصة بالقطاع الحكومي، ومنها ما هو عالمي أو محلي.

أمام أهمية التشفير، في تحقيق أمن المعلومات، تراجعت الدول عن مواقفها السابقة في تنظيمه، والتي كانت تخضعها لرقابة مشددة، أو تحظر نقلها. ففي العام ١٩٩٧، عدلت بلجيكا قانون ١٩٩٤، لتلغي الشروط الخاصة باستخدام التشفير. كذلك تخلت فرنسا، عن سياسة الرقابة التي مارستها على استخدام التشفير، في العام ١٩٩٩، معلنة حق الجميع في استخدامها. كما ألغت الولايات المتحدة الأميركية، الشروط الخاصة بمنع استيراد وتصدير هذه التقنية، في العام ٢٠٠٠.

وقد أعطت اللجنة الأوروبية، أمثلة عن الأشكال التي يمكن للتقنيات المستخدمة في التشفير ان تتخذها فأوردت: الاخفاء الأوتوماتيكي للأسماء في البيانات الشخصية، والتشفير لتسهيل عمل المسؤول عن معالجة البيانات الشخصية، وتقنيات منع الكعكات من اعطاء أوامر للجهاز، دون علم مستخدمه[118].

لكن إقرار مبدأ شرعية التشفير، الذي يدعمه ويطالب به المدافعون عن الحق في الخصوصية، ويرون فيه سلاحا لدعم الحرية والديمقراطية؛ كونه يؤمن حرية تبادل المعلومات، لاسيما في مجال اخفاء مضمون رسائل الناشطين، في حركات حماية حقوق الانسان، يحمل معه خطر استخدامه في الأعمال غير الشرعية، حين يساعد على اخفاء آثار مرتكبيها، وعلى اتصال أفراد العصابات والتنظيمات الإرهابية، أو الإجرامية الاخرى، ببعضها، بعيدا عن أعين الرقابة.

[116] *The 1997 OECD Guidelines on Cryptography Policy*
[117] *The 1998 European Commission report*
[118] *Des exemples de technologies donnés par la Commission européenne : l'anonymisation automatique de données ; le cryptage pour améliorer le travail du responsable du traitement des données à caractère personnel afin d'éviter le piratage ; les procédés anti-cookies, bloquant les cookies placés sur le PC pour faire exécuter à l'ordinateur des instructions à l'insu de l'utilisateur, les personnes concernées devant être informées du traitement en cours.*

فمن المعروف، أن المواقع التي تتولى الترويج للإرهاب، أو للاعمال الجهادية، كما يطلق عليها أصحابها، توزع تعليمات خاصة، حول استخدام هذه التقنية، كما توصي باستخدام البرامج التي تؤمنها. ويهتم العديد من المواقع على الانترنت، بالترويج لهذه البرامج ونشرها، ما يجعل امكانية استخدامها، متاحة للجميع[119]. وكان منتدى "الجبهة العالمية الاسلامية للإعلام»، قد تولى الإعلان عن إطلاق برنامج خاص للتشفير، أطلق عليه اسم "أسرار المجاهدين"[120]. كما قام العديد من المنتديات التي تدعم نشاطات إرهابية، بالترويج لهذا البرنامج[121]، الذي يحتوي على كتيب تعليمات، باللغة العربية، حول كيفية استعماله.

[119] *http://www.vicman.net/lib/encryption.htm*
[120] *Global Islamic Media Front Releases "Mujahideen Secrets", http://thesaloon.net/blog/CrimeLaw/_archives/2007/1/4/2620252.html*
[121] *SHAUN WATERMAN, " iDefense Director of Threat Intelligence Jim Melnick told UPI that «Mujahedin Secrets» was being «heavily promoted» on forums and other Web sites used by supporters of Islamic terror groups".http://www.upi.com/SecurityTerrorism/view.php?StoryID=20070129-053607-9471r*

﴿الفصل الخامس﴾
«الحرب السيبرانية» أو «الحرب الإلكترونية»

١ . علاقة وثيقة وحيوية

ارتبطت تقنيات المعلومات والاتصالات بالمجال العسكري، إذ تعود جذور الاستخدام الأول لشبكة المعلومات العالمية، إلى هذا المجال، بعد اكتشاف الأميركيين، أنها أحد أهم أسباب تفوق الروس عليهم، في أبحاث الفضاء وبعض الأبحاث الاخرى. وقد ازدادت أهميتها بعد اندماجها بوسائل الاتصالات وتوسعها، ودخولها في صناعة الأسلحة التقليدية، وعمليات تطويرها. وأثبتت قدرتها كذلك، في إدارة العمليات العسكرية.

وتعاظم شأن تقنيات المعلومات والاتصالات في هذا المجال، مع ترسخها كعنصر من عناصر منظومة الأمن الشامل، التي تتكون من القوة الصلبة؛ أي جميع العتاد والعديد العسكري التقليدي، والقوة الناعمة، أي " تجهيزات ومعدات الاتصال الحديثة، وتوفير المعلومة، التي أصبحت العصب الرئيس، الذي يُقاس تقدُّم أي بلد به. فبعد أن كان تقدُّم الأمم في القرن العشرين، يُقاس بالقدرة على التصنيع، أصبح يُقاس في القرن الحادي والعشرين، بالسرعة في الحصول على المعلومة، واستخدامها، وتوظيفها[122]».

وهكذا، شهد العالم، ولا يزال، تحولات جذرية وأساسية، في نماذج التعامل الاجتماعي والممارسة المهنية، نتيجة هذه الاستخدامات. وتحولت الانترنت، إلى بنية تحتية عالمية للنشاطات المدنية والعسكرية، والى وسيلة جديدة للضغط السياسي، والتجسس، ما فرض بعدا أمنيا جديدا، على اهتمامات الدفاع، لدى معظم حكومات العالم. وتصدر الأمن السيبراني، المراتب الأولى، في سياسات واستراتيجيات الدول الكبرى، الحريصة على نظامها، وامنها القومي، ومجتمعها، وسلامة مواطنيها.

٢ . توقعات كارثية

لا يخرج المجتمع الرقمي عن مبدأ «ان المجتمع هو الذي يهيئ أرضية الجريمة، اذ انه يحمل بذور الجرائم، التي يمكن ان ترتكب، كما الظروف، التي يمكن ان تساعد في توسعها وتطويرها[123]». وإذا كانت نتائج الجرائم السيبرانية، التي تطاول الأفراد والمؤسسات، ليست الا شكلا جديدا من اشكال الجريمة التقليدية، تماما كالاعتداءات التي تطال الأنظمة والدول، كاعمال التجسس، والتشويش على الاتصالات، واختراق الأنظمة المعلوماتية، الا ان آثار هذه الجرائم والاعتداءات، مرتبطة بطبيعة البيئة الرقمية. من هنا، فانها تجنح إلى اتخاذ صفة كارثية، لا يمكن تصورها، نظرا لحجم امتداداتها غير المحدودة، وتنوعها.

[122] أ- د. عادل طويسي. أمين عام المجلس الأعلى للعلوم والتكنولوجيا/ وزيرالثقافة السابق في المملكة الأردنية الهاشمية- الأمن السيبراني والهوية الوطنية ومنظومة الأمن الوطني الشامل- المؤتمر الدولي الثالث حول القانون السيبراني: الملكية الفكرية، وحماية البيانات الشخصية والأمن الوطني- الجمعية اللبنانية لتكنولوجيا المعلومات 22-20 / - تشرين أول (أكتوبر)- 2000 – تنظيم الجمعية اللبنانية لتكنولوجيا المعلومات- بيت المحامي- بيروت - لبنان

[123] *Society contains the germs of all the crimes that will be committed, as well as the conditions under which they can develop. It is society that, in a sense, prepares the ground for them, and the criminal is the instrument ... AdolpheQuetelet on crime.*

وإذا اضفنا، إلى ما تقدم، واقعة العمل المتواصل، من قبل الاقمار الصناعية، والشبكة العالمية للاتصالات، على رصد، وبث تحرّكات المواطنين والسلطات على السواء، فاننا ندرك خطورة الامر، أكثر فأكثر، كما ندرك أهمية إقرار المسؤوليات، عن أي ضرر أو تعرض للحقوق، يحصل نتيجة ذلك.

ويمكننا رؤية المدى الكارثي، لهذه الاعتداءات، في السيناريو الذي تخيله حمدون توري، الامين العام للاتحاد الدولي للاتصالات، في « البحث عن السلام السيبراني» في العام ٢٠١١، حيث تأتي الهجمات دون مقدمات، وحيث تعم الفوضى، وتنهار جميع الخدمات، التجارية، والحيوية، والصحية، والعسكرية، والحكومية، نتيجة لها، بما يشبه أفلام الخيال العلمي[124].

لا شك اننا لا نستطيع الجزم، بصحة اي من التوقعات، لكن القياس على ما حصل من هجمات، حتى الآن، يؤكد على ضرورة اتخاذ خطوات وإجراءات وقائية، وتحضير خطط هجومية، في حال الضرورة.

٣. هاجس الحرب السيبرانية

أمام هذا الواقع، تتحول مخاوف الدول من الاعتداءات ووقعها المحتمل، إلى هاجس اسمه الحرب السيبرانية[125]. وقد برز هذا الهاجس، بشكل واضح، في حديث البعض عنها، وكانها الحرب العالمية الثالثة. و لم يتوان العديد من القيادات العسكرية والسياسية، عن توقع بيرل هاربر[126] جديد، يتمثل في الهجمات السيبرانية.

تعطى الحرب السيبرانية تعريفات تستند أولا إلى البيئة، التي تتم فيها عمليات الاعتداء، فنجد مثلا تعريفا يعتبرها «صراعات واعتداءات ترتكز على الانترنت، وتحركها أهداف سياسية على المعلومات وأنظمتها، ويمكنها ان تؤدي فيما تؤدي، إلى وقف الخدمات الأساسية، وسرقة معلومات سرية، وشل النظام المالي، تعطيل المواقع الرسمية وشبكات الاتصال»[127].

فبالرغم من جهود المنظمات الدولية، وبعض التحالفات الاقليمية والعديد من الخبراء، إيجاد تعريف موحد للحرب السيبرانية، لم يتم حتى اليوم، التوصل إلى نتيجة حاسمة. ويعود ذلك، إلى اختلاف طبيعة استراتيجيات الدول وأهدافها، والى اختلاف مرتكزات التعريف، حيث تعتمد الولايات المتحدة الأميركية وحلفائها، مقاربة اقتصادية ومادية لا وجهها، بينما تركز منظمة شنغهاي للتعاون، على أهداف الصراع في الفضاء السيبراني، مثل: السيادة الوطنية، والهوية الثقافية. وهكذا خرجت مجموعة

[124] حمدون توريه- البحث عن السلام السيبراني- -2011 «أصبحت تكنولوجيا المعلومات والاتصالات جزءاً لا يتجزأ من الحياة اليومية لكثير من الأشخاص في أنحاء العالم. والاتصالات الرقمية والشبكات والأنظمة تقدم موارد حيوية وتمثل بِنية تحتية لا غنى عنها في كل جوانب المجتمع العالمي، وهي ضرورات لا يمكن لكثير من سكان العالم الازدهار أو حتى البقاء بدونها. وهذه الهياكل والأنظمة تمثل ميداناً جديداً تقترن به تحديات جديدة للحفاظ على السلام والاستقرار. وبدون آليات كفالة السلام فإن مدن العالم ومجتمعاته ستكون عرضة لهجمات تتسم بتنوع غير مسبوق وغير محدود. وهذه الهجمات يمكن أن تأتي دون مقدمات. فالحواسيب والهواتف الخلوية تتوقف عن العمل فجأة كما أن شاشات آلات صرف النقد والآلات المصرفية تنطفئ في وجه العملاء وتتعطل أنظمة مراقبة الحركة الجوية والسكك الحديدية وحركة السيارات وتعم فوضى الطرق السريعة والجسور والممرات المائية وتتوقف السلع غير المعمرة بعيداً عن السكان الجائعين. ومع اختفاء الكهرباء تهوي المستشفيات والمساكن والمراكز التجارية بل ومجتمعات بأكملها في غياهب الظلام. ولن تستطيع السلطات الحكومية معرفة مدى الضرر أو الاتصالات ببقية العالم لإبلاغه بالكارثة أو حماية مواطنيها الضعفاء من الهجمات التالية. وهذه هي المحنة القاسية التي يواجهها مجتمع تعرض للشلل بسبب ضياع شبكاته الرقمية في لحظة واحدة. وهذا هو التدمير الذي يُمكن أن ينجم عن نوع جديد من الحروب هي الحرب السيبرانية

[125] أي: أساليب الحرب ووسائلها التي تعتمد على تكنولوجيا المعلومات، والتي تستخدم في سياق نزاع مسلح

[126] *The secretary of defense, Leon Panetta: "The next Pearl Harbor we confront could very well be a cyber attack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems,". http://www.huffingtonpost.com/2011/06/13/panetta-cyberattack-next-pearl-harbor_n_875889.html*

[127] *Cyberwarfare is Internet-based conflict involving politically motivated attacks on information and information systems. Cyberwarfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and criple financial systems -- among many other possibilities. - http://searchsecurity.techtarget.com/definition/cyberwarfare*

الخبراء في الناتو بتعريف الحرب السيبرانية على انها: «جميع العمليات السيبرانية سواء أكانت دفاعية، أو هجومية، والتي يمكن ان تسبب اصابات أو وفيات، أو تلف وأضرا ر مادية[128]».

وهنا، نلاحظ اغفال هذا التعريف، للعنصر الأهم في أمن المعلومات، أي العامل البشري النفسي، ما يجعله غير ملائم لأشكال الاشتباك والصراع الحاليين، لاسيما وانه لا يمكن الاعتماد عليه، للتمييز الواضح، بين الحروب السيبرانية وحروب المعلومات، وبين أشكال الجريمة السيبرانية والإرهاب السيبراني، كما انه لا يساعد على تبيان الحدود الفاصلة بينها. وفي ذلك، تحديات تطاول تحديد امكانيات واشكال التنسيق المفروض اعتمادها، كما طبيعة ونوعية مهمات عناصر القيادة والتحكم بالقطاعات العسكرية، والاقتصادية والمدنية.

إذا، وفي غياب التعريف الموحد، تبدو هذه الحرب عمليا، كامتداد لحرب الاستخبارات، وكميدان جديد للنزاعات، يأخذ مكان الحرب الباردة. أما مميزاتها، فهي انها سرية، خفية، ومحاطة بالكثير من المغالطات والتضخيم.

في الحقيقة، ان معظم الاعتداءات السيبرانية، لا تحدث أضرارا مادية، يمكن لمسها. فطبيعة الفضاء السيبراني، والمصالح المتصلة به، شديدة التعقيد، نظرا لامتدادات البنية التحتية، وتشابكها، ونظرا للتقنية العالية، وسرعة تطورها، وامكانات تمويه مصادر الاعتداءات. هذا عدا، عن صعوبة تحديد ما الذي يمكن اعتباره عملا عسكريا، أو اعتداء، او حربا سيبرانية. فالسرقات التي تطال المصارف، وعمليات التجسس الصناعي، ليست اعمالا حربية، بالرغم من ابعادها الخطرة، على الامن القومي، لانها تمس بالاقتصاد الوطني، ورفاه البلد. الا أن الخبراء يرون، انعكاسات الاعتداء على البنك المركزي الأميركي، مثلا، أشد وأدهى، من اعتداءات الحادي عشر من سبتمبر،على الاقتصاد العالمي[129].

فلم تتسبب الهجمات السيبرانية على أستونيا، وجورجيا، وإيران، بأضرار بشرية، و لم تذكر لها نتائج خطيرة على المدنيين، ولكن يمكننا تصور نتائجها الوخيمة على السلام، لو اعتبرت هذه الاعتداءات حربا، كونها استهدفت تعطيل مواقع ومصالح حيوية، ومنها تلك الخاصة، بالقوات المسلحة، أو فيما لو اعتبرت الهجمات، من فعل جيش سيبراني معين، استخداما للقوة.

فبالرجوع إلى قواعد العلاقات الدولية، نجد مبدأ «الامتناع عن استخدام القوة»، حفظا للسلم والاستقرار الدوليين، كقاعدة ملزمة، تترتب على مخالفتها، نتائج قانونية.

وقد نصت المادة الثانية من الفقرة الرابعة، من ميثاق الأمم المتحدة على أنه: «يمتنع أعضاء الهيئة جميعا، في علاقاتهم الدولية، عن التهديد باستعمال القوة، أو باستخدامها، ضد سلامة الأراضي، أو الاستقلال السياسي لأية دولة، أو على وجه أخر لا يتفق ومقاصد الأمم المتحدة. وإذا كانت الاجتهادات الكثيرة، قد ارفقت «القوة» بعبارة المسلحة، الا ان روح الاتفاقية واضحة، فيما يتعلق بمنع اللجوء إلى القوة،

[128] *https://www.icrc.org/ara/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm*
[129] *La guerre cybernétique, nouveau prétexte des pressions anti-iraniennes!.dimanche, 21 octobre 2012 04:44 « Bien qu'une guerre cybernétique ne soit pas aussi destructrice et dévastatrice qu'une guerre militaire, cependant, si la seule grande banque des Etats-Unis fait l'objet d'une telle attaque, ses impacts seront beaucoup plus importants, pour l'économie mondiale, que ceux de l'attentat du 11 septembre 2001, selon les analystes américains». http://french.irib.ir/analyses/commentaires/item/220167-la-guerre-cybern%C3%A9tique,-nouveau-pr%C3%A9texte-des-pressions-anti-iraniennes*

بغض النظر عما إذا كان من خلال القوات المسلحة، أم غيرها من الأساليب. والدليل على ذلك، هو عنوان الفصل السابع، من الشرعة نفسها: « فيما يتخذ من الأعمال في حالات تهديد السلم والإخلال به ووقوع العدوان». وعليه، فان الأعمال المخلة بالسلم، والمهددة له، هي ممنوعة أيضا، ويمكن الرد بالتالي، على اي اعتداء. وإذا كانت الشرعة، لم تحدد المقصود «بالأعمال المخلة بالسلم» أو "الأعمال المهددة للسلم» أو «الأعمال العدائية»، الا ان المتفق عليه، هو ان هذه الأعمال، هي كل عمل يتعارض مع أهداف المجتمع الدولي، في تحقيق السلام، والمبادئ التي يجب ان ترعاها.

وكانت الجمعية العمومية للأمم المتحدة، قد اتخذت قرارا تحت الرقم A/ARES ٣٣١٤/ الدورة ٢٩ /١٩٧٤، عرفت فيه العدوان، وربطته باستعمال القوة المسلحة، حيث جاء في المادة الأولى؛ "العدوان هو استعمال القوة المسلحة، من قبل دولة ما ضد سيادة دولة أخرى...". وعددت الأعمال التي تنطبق عليها هذه الصفة، في المادة الثالثة، معتبرة في المادة الرابعة، ان الأعمال المعددة اعلاه ليست جامعة مانعة، ولمجلس الأمن ان يحكم بان اعمالا اخرى تشكل عدوانا بمقتضى المادة الميثاق. وطالما ان قرار الجمعية غير ملزم، وطالما ان مجلس الأمن هو صاحب القرار وبشكله الملزم، حسب الفصل السابع، فان بامكانه اعطاء توصيف لعمل "عدواني"، ليس مرتبطا باستعماله القوة المسلحة.

ومعلوم ان قرار الجمعية العمومية، يندرج في سياق تاريخي محدد اي السبعينات، حيث لم تكن تكنولوجيا المعلومات والاتصالات، قد برزت بالقوة التي نشهدها اليوم، ولم يكن استعمالها يطاول كامل اوجه الحياة تقريبا.

كما تسجل أيضا، مواقف البعض، من ان الحرب السيبرانية، هي الحرب التي لا حدود لها، ولا ضوابط، فالمعلومات في كل مكان، وساحة المعركة في كل مكان، وامكانات الجمع بين التقنيات المختلفة متوفرة، والحدود بين الحرب واللا حرب، لم تعد موجودة[130].

٤. أدوات الحرب السيبرانية

وتشكل الفيروسات الأسلحة الأساسية في الحرب، حيث تؤدّي إلى تعطيل عمل الشبكات الإلكترونية، والخوادم الرئيسية Servers، أو تؤدي، إلى استخدامها لإرسال مختلف المعلومات، من الأماكن التي تغزوها. ويمكن نشر الفيروسات، عبر الرسائل الإلكترونية، أو نقل الملفات الإلكترونية، أو تحميلها على أداة لحفظ البيانات. ويُشار هنا، إلى أنّ فيروس «Stuxnet»، الذي ضرب المفاعل النووي الايراني، قد تم، عبر استخدام هذه الطريقة الأخيرة «USB»، لاسيما وان هذا المفاعل، غير موصول بالشبكة العنكبوتية العالمية.

ولا تقتصر الحرب الإلكترونية، على الفيروسات والبرامج المعادية، فهي تشمل أيضا التشويش المادي المباشر، المتعلق بموجات البث السلكي اللاسلكي، وشبكات الطاقة. ولا شيء يمنع، أن يتحوّل الرد على هجوم سيبراني، إلى هجوم عسكري مباشر.

[130] *1- Unrestricted Warfare»: Military/Civilian Distinctions Break Down - « Unrestricted Warfare» means that any methods can be prepared for use, information is everywhere, the battlefield is everywhere, and that any technology might be combined with any other technology, and that the boundaries between war and non-war and between military and non-military affairs has systematically broken down. [pp. 6-7] - http://www.fas.org/nuke/guide/china/doctrine/unresw1.htm*
2 - *cyber guerre et guerre de l'information- Hermes Lavoisier 2010- p :164" la première règle de la guerre hors limite est qu'il n'y a pas de regles, rien nést interdit... il n'y a rien dans le monde aujourd'hui qui ne puisse devenir une arme »*

وفي هذا السياق، ذكرت صحيفة The Daily Beast الأميركية، أن أي هجوم إسرائيلي على إيران سيكون مدعوماً بغارات إلكترونية، من الفيروسات، إضافة إلى عمليات التشويش. فقد تمكنت إسرائيل من تطوير التقنيات اللازمة، لايقاف شبكة الهاتف الايرانية، مع امكانية تعطيل نظام الإنذار لديها، ومنعه من بثّ الرسائل اللازمة، بعد هجمة استباقية، تشنها الطائرات مثلاً[131]. ولا يعتبر هذا السيناريو خياليا، فقد تمكنت اسرائيل من تعطيل الرادارات السورية، لدى اغارتها وقصفها، على موقع الكبر النووي السوري، قرب دير الزور.

ويلاحظ دخول العديد من الدول، وإن بصورة خفية، مجال الأعمال الاستخباراتية السيبرانية، والاختراقات المتبادلة لأنظمة المعلومات.

ففي العالم العربي، تعرض العديد من المواقع الخاصة بجهات أمنية، ووزارات مهمة، الى اعتداءات، واختراقات[132]،وتوقف العمل فيها، لعدد من الساعات. وفي هذا الإطار، صرح القائد السابق لسلاح الجو في الامارات العربية المتحدة، إن البنية التحتية الإلكترونية المتقدمة في بلاده، جعلتها هدفا مفضلا للمتسللين عبر الانترنت، خاصة لدى تصاعد التوتر، في الصراع الفلسطيني الاسرائيلي[133].

كذلك، فقد تعطّلت شبكة «أرامكو» السعودية، التي يعمل عليها ٣٠ ألف جهاز حاسوب، وهدّدت بإعاقة قدرات إنتاج نحو ٩ ملايين برميل يومياً، للسوق العالمية – بسبب أحد الفيروسات الإلكترونية: «شامون». ويجزم الخبراء، من روسيا إلى الولايات المتّحدة، بأن هذا الهجوم، هو جزء من الحرب الإلكترونية، التي تزداد ضراوة في الشرق الأوسط. وقد استهدف هذا الهجوم، إضافة إلى المملكة العربية السعودية، شبكات الغاز القطرية. وقد توجهت الاتهامات،في هذه الحادثة، إلى إيران[134].

وكانت هذه الأخيرة، قد تعرضت لهجوم فيروسين، اعتبرا الاقوى، والأكثر حيلة، وقدرة على الاختراق، هما: Flame وStuxnet. فقد حول الأول الأجهزة الايرانية، إلى آلات تصوير وتسجيل، ومراقبة، وأوقف العمل، في مرفأ «خرج» النفطي، ما أدى إلى فصله عن الشبكة الإلكترونية، بينما أوقف الثاني، عمل مئات من أجهزة الطرد المركزي، في معامل تخصيب اليورانيوم.

وتوجّهت أصابع الاتهام مباشرة، إلى إسرائيل والولايات المتّحدة اللتين لم تنفيا التهمة[135]. بعد ذلك، ظهر فيروس «غوس» (Gauss)، الذي ضرب في لبنان، وإسرائيل، والأراضي الفلسطينية. وقد أوضحت حينها شركة «Kaspersky» الروسية، أنّ «غوس» قادر على سرقة المعلومات الشخصية من الحواسيب التي يهاجمها[136]، وهو قادر أيضا على التجسس، على العمليات المصرفية المختلفة.

كذلك، تعرض كل من لبنان وإيران، لما سُمّي بفيروس «MiniFlame»، وهو نسخة معدّلة، عن الفيروس "Flame". ويستخدم هذا الفيروس، لشن هجمات محددة الأهداف، مثل سرقة البيانات، واختراق الأنظمة.

---

[131] *Israel's Secret Iran Attack Plan: Electronic Warfare- Nov 16, 2011 6:28 PM EST - http://www.thedailybeast.com/articles/2011/11/16/israel-s-secret-iran-attack-plan-electronic-warfare.html*

[132] تعرض مواقع إلكترونية سعودية للهجوم - *http://www.aleqt.com/2013/05/19/article_756759.html*

[133] تصاعد الهجمات على البنية التحتية في الخليج: *http://human.iraqgreen.net/modules.php?name=News&file=article&sid=32757*

[134] *In Saudi Arabia and Israel, Signals That Iran Has Retaliation in Works- Oct 26, 2012 4:45 AM EDT http://www.thedailybeast.com/articles/2012/10/26/in-saudi-arabia-and-israel-signals-that-iran-has-retaliation-in-works.html*

[135] *Sorry, Iran. I Didn't Mean to Invade You. Jul 17, 2012 4:29 PM EDT. http://www.thedailybeast.com/articles/2012/07/17/sorry-iran-i-didn-t-mean-to-invade-you.html*

[136] أسماء المستخدمين وكلمات السر للدخول إلى النظام، والى البريد الإلكتروني وشبكات التواصل الاجتماع

ويعتقد بعض الخبراء، أن الفيروس الذي استهدف لبنان، اختصّ بسرقة بيانات مصرفية حساسة، كانت وراء العملية «Titan»[137]، التي قامت بها الولايات المتحدة الأميركية، من خلال وزارة المال الأميركية، بالتعاون مع أجهزة الاستخبارات، والتي اسفرت عن اتهام البنك اللبناني الكندي، بتبييض الأموال لصالح حزب الله. وقد أدى الاتهام، كما هو معروف، إلى تصفية أعمال المصرف، واغلاقه.

في المقابل، تعرضت كبرى المصارف الأميركية[138]، إلى هجوم لم تستطع السلطات منعه، نظمته مجموعة من القراصنة الإيرانيين، المدعومين حكومياً، تُسمّى «مقاتلو القسّام الإلكترونيون».

كذلك، تواجه الولايات المتحدة الأميركية، هجمات تشنها الصين، بهدف التجسس، على شبكات إلكترونية حكومية، ومراكز ابحاث، وشركات كبرى.

وتُصنّف تلك المجموعات، على أنها جناح من المجمع الصناعي العسكري الصيني، المسمى «المركز الشمالي للكمبيوتر في بكين». كذلك تتعرض الولايات المتحدة، لحملات تشنها مجموعات مدنية، من القراصنة الروس، وصولاً إلى شبكة الثورة العالمية Anonymous فضلاً عن الجيش العربي الإلكتروني.

على ضوء ما تقدم، تحشد حكومات عديدة، جيوشا من الخبراء المعلوماتيين، وتخصص موازنات طائلة، لضمان سلامة انظمتها، وأمن بياناتها، في مواجهة الاختراقات، والاعتداءات المختلفة.

وتترافق هذه الإجراءات، مع حركة ناشطة، على المستوى الدولي، لحث الدول قاطبة، على الالتزام بثقافة الأمن السيبراني، تقودها الهيئات الدولية، وفي مقدمها الأمم المتحدة، والاتحاد الدولي للاتصالات، ومنظمة التعاون الاقتصادي والتنمية، والاتحاد الأوروبي، وهيئة إدارة أسماء النطاقات، وأكثر الذين يصدرون الدراسات، والاستراتيجيات والسياسات والارشادات، والقرارات ذات الصلة.

وفي هذا المجال، قال اللواء المتقاعد البوعينين، في تصريح، على هامش مؤتمر للأمن الإلكتروني في دبي: "هناك اهتمام على المستوى السياسي، بالأمن الإلكتروني لحماية مصالح الناس، والحكومة، والأمن القومي أصبح معتمدا على هذا الموضوع[139]».

[137] *Statement of Celina B. Realuyo* Professor of Practice William J. Perry Center for Hemispheric Defense Studies On Hezbollah's Global Facilitators in Latin America At a Hearing Entitled "Terrorist Groups in Latin America: The Changing Landscape" Before the Subcommittee on Terrorism, Non-Proliferation, and Trade House Committee on Foreign Affairs, U.S. House of Representatives February 4, 2014 - http://docs.house.gov/meetings/FA/FA18/20140204/101702/HHRG-113-FA18-Wstate-RealuyoC-20140204.pdf*

[138] *Banks Seek U.S. Help on Iran Cyberattacks - January 15, 2013, 7:31 p.m. EThttp://online.wsj.com/article/SB10001424127887324734904578244302923178548.html*

[139] *http://human.iraqgreen.net/modules.php?name=News&file=article&sid=32757*

٥. الاستثمار في المجال التقني

ترتكز معظم استراتيجيات الحماية والدفاع، في المجال السيبراني، على مقاربة ثلاثية الأبعاد: الحد من المخاطر، استكشاف الإمكانات، وتعزيز امكانات التعامل السريع مع الطوارئ.

بناء على ذلك، لا بد من الإحاطة بمكامن الخطر، وتحديد نقاط الضعف، والحد من أبعاد الاعتداءات. ويفسر هذا الامر عمليا، بجمع المعلومات، ومعالجة البيانات، والترويج لسياسة الحكومة، في مجال الأمن والسلامة، واتخاذ الخطوات الضرورية، للرد على العدو، وعلى الاعتداءات عند الحاجة. وبما ان هذه الخطوات جميعها، تفترض وجود اجهزة متخصصة، وخبرات متمكنة، يبدو واضحا ضرورة الاستثمار، على المستوى التقني، عبر اعتماد تقنيات متطورة، وعلى المستوى الاداري، عبر التمكين والتدريب، ونشر المعرفة، وتحسين عملية الإدارة، وآليات اتخاذ القرار، بما يتناسب وطبيعة المخاطر وحاجات التدابير، والعمليات العسكرية السيبرانية.

وعلى سبيل المثال، يعتبر رصد نقاط الضعف في البرامج، من الضرورات، على مستوى تامين الحماية، للأنظمة والمواقع. ويمكن لهذا الامر، ان يؤمن حماية من بعض الاختراقات، كتلك التي استهدفت مثلا، موقع الأمم المتحدة، وموقع شركة مايكروسوفت، عبر SQL Injection، وهي نقطة ضعف، كان من الممكن تفاديها.

ولعل الدليل الأبرز على أهمية هذا الامر، هو استثمار الأجهزة الأمنية، في الولايات المتحدة الأميركية، في هذا المجال[140]، بحيث تقوم بشراء المهارات، والمعلومات الخاصة، بنقاط الضعف في البرامج والتطبيقات، الأكثر انتشارا، حول العالم، كخطوة احترازية، تمنع استغلالها من قبل الأنظمة الدكتاتورية، والمنظمات الإرهابية.

وتستثمر الحكومة الصينية، هي الاخرى، في هذا المجال أيضا. وذلك من خلال المبرمجين، والمتخصصين الوطنيين، لديها.

أ- الموازنات العسكرية: نموذجا

يأتي إقرار الموازنات العسكرية، في إطار استراتيجيات الدولة، سواء الدفاعية منها أم الهجومية، وعلى ضوء الحاجات التي تفرضها هذه الاستراتيجيات، والمهمات المطلوبة من القوى العسكرية. لذا، تعكس الموازنات، الاهتمامات والأولويات، لدى كل حكومة وجهاز وإدارة.

وهكذا يلاحظ اليوم، إقرار بنود في الموازنات العسكرية تسمح، ليس فقط بالحصول على الأسلحة التقليدية المطورة معلوماتيا، وانما أيضا، بتطوير برامج معلوماتية واتصالات، تمكن الجيوش من ممارسة دورها، في حماية الأمن القومي، في المجالين المادي والسيبراني.

ويذكر في هذا المجال، تخصيص نصف مليار دولار، من موازنة الاستثمار في الفضاء السيبراني، من

[140] *Special Report: U.S Cyber war strategy strokes fear of blowback- "...Computer researchers in the public and private sectors say the U.S. government, acting mainly through defense contractors, has become the dominant player in fostering the shadowy but large-scale commercial market for tools known as exploits, which burrow into hidden computer vulnerabilities. In their most common use, exploits are critical but interchangeable components inside bigger programs. Those programs can steal financial account passwords, turn an iPhone into a listening device, or, in the case of Stuxnet, sabotage a nuclear facility".http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510*

قبل وزارة الدفاع الأميركية، لأغراض البحث عن برامج وتطبيقات عسكرية، لاسيما في مجال تشفير المعلومات، بما يؤمن حماية المصالح الأميركية السيبرانية[141].

لذا، تضع بعض الدول الحرب السيبرانية، على سلم أولوياتها الإستراتيجية الوطنية، لحماية الأمن القومي. وتجهد العديد منها، في دراسة وتبيان، حجم الموازنات العسكرية، ومدى اعتمادها على تقنيات المعلومات والاتصالات، كمؤشر على قدراتها ومؤهلاتها السيبرانية[142]. ويعتبر الاستعلام، والاستخبار، والتجسس، وقطع اتصالات العدو، والتشويش عليها، والتنصت، من المبادئ في العمليات العسكرية، وكمكمل للحرب الإلكترونية، وعمليات الاستعلام.

وتعتبر بعض الدول متقدمة جدا، كونها تستخدم عددا وعديدا من اصحاب الكفاءات، للاهتمام بوضع استراتيجيات دفاعية وهجومية سيبرانية، كجزء من امكاناتها العسكرية، لمواجهة الحرب السيبرانية، كما تعمل على تطوير تقنيات، تساعدها على تمييز الهجمات العسكرية، من الاعتداءات والاختراقات الجرمية العادية. وتلجأ اخرى، إلى ربط امكاناتها العسكرية السيبرانية، بما هو متوفر لديها، من تخطيط للحرب التقليدية. الا أن هذا الربط يستدعي، فيما يستدعي، انتباها خاصا، إلى توسع مروحة وسائل الاتصالات، والشبكات، ونقاط الوصول اليها، والتحول نحو الاتصال غير السلكي والجوال. mobile and wireless

وفي الدول التي ما زالت تعتمد على النمط القديم، الذي ظهر في التسعينيات من القرن الماضي، اوكل الأمن السيبراني، إلى مراكز الرد على طوارئ الانترنت الوطنية، (CERT)، ووزارة الاتصالات، أو وزارة التكنولوجيا، والى وحدات خاصة ضمن الأجهزة الأمنية لديها. وواضح، ان هذا النمط، لا يمكنه مجاراة النمط المتقدم، لأسباب عديدة، ليس أقلها، ما يوفره هذا الأخير، من قدرة على إدارة الشؤون السيبرانية، بصورة أشمل وأسرع، من قبل الجهة المعنية بالدفاع مباشرة.

وبالرغم من تخفيض قيمة الموازنة العسكرية، لحظت الموازنة المقترحة للعام ٢٠١٤، في الولايات المتحدة الأميركية، زيادة لصالح الحرب السيبرانية، بلغت حوالي البليون دولار، وذلك بهدف توسيع قدرات الدفاع السيبرانية، بحيث تشمل العمليات العسكرية، امكان اغلاق نظام القيادة لدى العدو، ومنع راداراته من التقاط أي حركة، وذلك في حال حصول حرب. وقد حرص المسؤولون على التشديد، على ان استخدام هذه القدرات، محصور ضمن حدود قانون النزاعات المسلحة[143].

وغني عن القول، ما تعنيه هذه الزيادة، من تحريك لعجلة الاقتصاد الأميركي، لصالح الشركات التي تتولى الابحاث، وتزويد البنتاغون بالبرامج والتطبيقات الأمنية، إضافة إلى المعدات والأسلحة، التي ترتكز إلى تقنيات الاتصالات والمعلومات.

---

[141] *Special Report: U.S Cyber war strategy strokes fear of blowback – "...DOD's cyber investment includes a half billion dollars in research funding for DARPA (Defense Advanced Research Projects Agency) in the last budget"-*
http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510

[142] *Cybersecurity and Cyberwarfare- Preliminary Assessment of National Doctrine and Organization- 2011- Center for Strategic and International Studies. www.unidir.org*

[143] *Under President's Budget, Cybersecurity Spending Increases- "We must... confront new dangers, like cyber attacks, that threaten our nation's infrastructure, businesses and people," President Barack Obama wrote in the introduction to the budget proposal. "The budget supports the expansion of government-wide efforts to counter the full scope of cyber threats, and strengthens our ability to collaborate with State and local governments, our partners overseas and the private sector to improve our overall cybersecurity."*
http://news.clearancejobs.com/2013/04/26/under-presidents-budget-cybersecurity-spending-increases/

٦ . التقنيات في العمليات العسكرية

في زمن تقنيات المعلومات والاتصالات، اختلف مفهوم العمليات العسكرية، فقد تبدل ميدان المواجهة، والهدف يمكن اصابته، من أي نقطة في العالم، وفي أي وقت، وتبدلت مع ذلك، قدرة الرد والدفاع، التي تفترض هي الاخرى، تحديدا لنقطة انطلاق الهجوم، وكذلك مراكز العدو. كما تأثرت القدرة على الرد السريع، وعلى إدارة النتائج، واثبات مصدر الاعتداء والمسؤولية.

وانصبت الجهود على حيازة الأسلحة الذكية، والأسلحة العاملة عن بعد، بحيث أصبح السلاح الذكي والمطور معلوماتيا، والموصول بشبكة معلومات، أساسيا في ترجيح الكفة أثناء الحروب. ويأتي بعدها العنصر البشري، الذي يتطلب هو الآخر، مجهودا لبنائه، وتمكينه. كذلك، فقد اختلف مجال العمليات العسكرية، وانتقل النشاط العسكري، كما النشاط الاجتماعي، والتجاري، والاقتصادي، إلى المجال السيبراني. وهكذا، تحتوي ترسانة العديد من الجيوش، على الأنظمة المعلوماتية، والمعدات الإلكترونية، التي تستخدم، سواء في إدارة الموارد البشرية، أم اللوجستية، أم خلال العمليات.

وتظهر التقنيات في المجال العسكري، على مستويات مختلفة. فإضافة إلى التقنيات المستخدمة في الأسلحة التقليدية، كالطائرات والدبابات، برزت تقنيات الرصد والاستعلام، وجمع البيانات بكل أنواعها، وبرامج التوجيه عن بعد، واستخدام الروبوت أو الإنسان الآلي في العمليات العسكرية، لإزالة الألغام وتوجيه الآليات عن بعد، والقيام بعمليات الاستطلاع، والاستكشاف الميداني.

يضاف إلى ذلك، ضرورة التنبه إلى عدم امكانية تحقيق الفعالية المرجوة، في مواجهة تهديد الحرب السيبرانية، دون مشاركة أصحاب المعارف المتخصصة، والفهم العميق للتقنيات، التي تغير الصورة على المسرح العالمي[144]، ما يعني الحاجة الماسة، إلى تأهيل العنصر البشري، وتدريبه، بصورة مستمرة، بما يتناسب مع حركة تطور الفضاء السيبراني، التي لا تهدأ.

ويبرز دور المعلوماتية، بشكلٍ خاص، في أنظمة التسلح، التي تساعد على استمرارية العمل القتالي، على مدار الساعة، ليلاً ونهاراً، وبغض النظر عن حالة الظروف الجوية، وذلك عبر تجهيزات الملاحة. والى جانب ذلك، أنظمة التسليح المخصصة للإطلاق البعيد Stand-off ذات الدقة العالية، والذخائر الذكية Smart Ammunition ذات التوجيه الذاتي، وأنظمة التسليح غير المأهولة Unmanned، والتي تسمح بالعمل في عمق دفاعات الخصم، في مجالي المراقبة والاستطلاع.

---

[144] البحث عن السلام السيبراني –حمدون إ. توريه- الأمين العام للاتحاد الدولي للاتصالات يناير 2011
http://www.google.com.lb/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&cad=rja&ved=0CC0QFjAA&url=http%3A%2F%2Fwww.itu.int%2Fdms_pub%2Fitu-s%2Fopb%2Fgen%2FS-GEN-WFS.01-1-2011-MSW-A.docx&ei=cjqgUcfQFbSf7AbTt4EI&usg=AFQjCNFJ9KhCOzjfH8zG-H3SIhfV_fot4g&sig2=5Ja6CXZVqhQJ_o2nko2BEg&bvm=bv.47008514,d.bGE

في هذا الإطار، يلاحظ مثلا، عمل وزارة الدفاع الأميركية، على تخصيص موازنات خاصة، لتمويل أبحاث تساعد على تحويل نصف مركباتها إلى مركبات آلية، تعمل دون وجود بشري على متنها، وذلك منذ عدة سنوات، كما تعمل على تطوير طائرات تجسس صغيرة الحجم، تستخدم النانو تكنولوجي، يمكنها اختراق أكثر الأماكن سرية، دون ان يتم رصدها. ويمكن تجهيز هذه الطائرات، بمعدات تنصت وتصوير، وأشعة ليزر قاتلة.

وتستخدم العديد من البرامج والتطبيقات، المصممة في الاساس لأهداف مدنية، في المجال العسكري. ويحضر هنا كمثال، برنامج "جوجل إيرث google earth" الذي يؤمن معلومات جغرافية، ويعرض صورًا للكرة الأرضية، وخرائط الدول، بتفاصيل دقيقة جداً، تصل إلى حد ابراز أسماء الشوارع، وأرقام المنازل، ما يساعد على تحديد الأماكن بسهولة كبيرة، ودقة متناهية، وبسرعة، مع توضيح خطوط الطول والعرض، للمناطق.

من هنا، يعتبر هذا التطبيق، على درجة من الاهمية، ومن الخطورة أيضا، كونه يساعد على كشف مناطق أمنية، لم يكن بالامكان كشفها في السابق، وذلك عبر الصور التي تلتقط، بواسطة الأقمار الصناعية. وهذا يجعل بعض المواقع مثل: الابنية الحكومية، والمراكز العسكرية، والمفاعلات النووية، أهدافا سهلة للهجوم وللاعتداءات، حتى فيما يعتبر عمليات حربية تقليدية.

وللتدليل على خطورة الامر، وامكانات الاستخدام العسكري لهذا التطبيق، نورد ما جاء في صحيفة التلجراف البريطانية، عن أن المسلحين في العراق، قد استخدموه، في تحديد المناطق التي استهدفوها، لتنفيذ هجمات، ضد المعسكرات البريطانية والأميركية.

على خط مواز، تعتبر أنظمة جمع المعلومات، مجالا حيويا من مكونات الترسانة العسكرية لجيوش البلدان المتقدمة، حيث يتيح إمكان الوعي بواقع ساحة المعركة، ليس من خلال المعلومات الإستخبارية فحسب، بل من خلال التأسيس لمفهوم التفوق المعلوماتي، بوصفه جوهر الثورة الحالية في الشؤون العسكرية. ومن أبرز مقوماته: تسخير الأنظمة الفضائية لجمع المعلومات، وجمع المعلومات الاستخبارية على المستوى الإستراتيجي في عمق أراضى الخصم، وتطوير القدرات الاستطلاعية التقليدية، لا سيما الجوية منها، بما يحقق استمرارية جمع المعلومات عن الخصم، والتكامل الأفقي بين أنظمة جمع المعلومات، وعملها بصورة متكاملة.

كما تساعد الأنظمة، في تعزيز آلية القيادة والسيطرة، وذلك عبر ربطها مراكز القيادة والسيطرة، وعبر الربط بينها وبين أنظمة جمع المعلومات في الوقت ذاته، على المستويات المختلفة. ويتيح هذا الربط إدراك القيادات المختلفة، لحقيقة ما يجرى في أرض المعركة، وبالتالي امكانية اتخاذ القرار المناسب، في الزمان والمكان الملائمين، بالنسبة للقوات الصديقة والعدوة، على السواء. كما تساهم في انسياب أوامر العمليات، وتنسيقها افقيا وعاموديا، وبين أجهزة وفروع القوات المسلحة، وقواتها المساندة اللوجستية، العاملة في مسرح العمليات.

ويساهم ما تقدم، فى دعم قدرة القيادات على المبادرة، بحيث لا يتأخر، رد الفعل المناسب.

٧. التقنيات ونماذج الإدارة

لحظت وزارة الدفاع الأميركية، في تقريرها الاستراتيجي حول الموازنة للسنة المالية ٢٠١٤، اعادة تنظيم، على مستوى الموارد البشرية والكفاءات لديها، لتعزيز قوتها السيبرانية، في مواجهة المخاطر[145]. وتلحظ الاستراتيجية، اعادة تنظيم القوة السيبرانية الحالية، ضمن فرق متخصصة، في مجالات ثلاث: حماية الشبكات، شلَ قوة العدو السيبرانية، وحماية الدفاع الوطني. وقد لحظت هذه الاستراتيجية، إنشاء قوة سيبرانية، بحلول السنة المالية ٢٠١٦، مؤلفة من اربعين فرقة، موزعة على مهمات هجومية، واخرى دفاعية.

وتتوزع مسؤولية الأمن السيبراني، في الولايات المتحدة الأميركية، حاليا، بين وزارة الداخلية، ومكتب التحقيق الفدرالي، ووزارة الدفاع، بما فيها قيادة الأمن السيراني، التي تضم وكالة الأمن القومي. وتسند العمليات الهجومية إلى هذه الأخيرة، إضافة إلى وحدات من وكالة الاستخبارات المركزية، بينما تتولى وزارة الداخلية، الأمن السيبراني على المستوى الداخلي، حيث تعمل وحدة الأمن القومي السيبراني فيها، بالتعاون مع القطاعين العام والخاص، ومع الهيئات الدولية، لحماية الفضاء السيبراني الأميركي، ومصالح أميركا السيبرانية. وتتولى هذه الهيئة، حماية البنية التحتية الوطنية، ضد الهجمات التي يمكن ان تتعرض لها، من خلال عدد من البرامج المخصصة لهذه الغاية. وتتولى مجموعة الاستجابة السيبرانية الوطنية، تنسيق الجهود على المستوى الفدرالي، في حال حدوث طارئ سيبراني وطني. وتعمل هذه المجموعة، تحت امرة إدارة الأمن السيبراني الوطني.

في المقابل، يتولى الجهاز القيادي السيبراني، التابع للقيادة الفدرالية، مسؤولية حماية البنية التحتية السيبرانية العسكرية. ويضم هذا الجهاز، القيادة السيبرانية التابعة للجيش، وقيادة القوات الجوية، والبحرية.

وتعمل وزارتا الدفاع والداخلية في الولايات المتحدة، على تنسيق جهودهما، بموجب اتفاق وقع بينهما، في اكتوبر ٢٠١٠، لتعزيز التعاون الداخلي بين مختلف الأجهزة، التابعة لكل منهما.

وكانت ايران، قد أعلنت عن تشكيل وحدة عسكرية خاصة بالأمن السيبراني، لمواجهة الاعتداءات السيبرانية[146]. كما تحدث العديد من التقارير، عن إنشاء الجيش الصيني السيبراني[147]، الذي وجهت اليه الاتهامات عن عمليات التجسس، وعن الاعتداءات التي طاولت مؤسسات حكومية، ومصرفية، ومالية، وأمنية، إضافة إلى شركات خاصة، في الولايات المتحدة الأميركية.

---

[145] *Defense Budget Priorities and Choices Fiscal Year 2014.http://www.google.com.lb/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&sqi=2&ved=0CCsQFjAA&url=http%3A%2F%2Fwww.defense.gov%2Fpubs%2FDefenseBudgetPrioritiesChoicesFiscalYear2014.pdf&ei=2FagUbXxKsmt4ATSzoGIBg&usg=AFQjCNGTTf1a9VAMRqoEnYCXY32wN25q4g&sig2=7c6aAXHNGjJpxoHDyxd4bg&bvm=bv.47008514,d.bGE*

[146] *Iran is building a non-nuclear threat faster than experts ‹would have ever imagined. http://www.businessinsider.com/irans-cyber-army-2015-3*

[147] *How China›s Night Dragon cyber army has infiltrated every corner of Britain: Forget Edward Snowden... a chilling new book by the BBC›s top security expert lays bare the biggest internet hack in history. http://www.dailymail.co.uk/news/article-3113736/How-China-s-Night-Dragon-cyber-army-infiltrated-corner-Britain.html*

٨. التعاون لدرء المخاطر

انطلاقا من الطبيعة الخاصة للفضاء السيبراني، تقر الدول والهيئات الدولية كافة، بضرورة التعاون، بين القطاعين العام والخاص، لدرء المخاطر السيبرانية. فالقطاع الخاص، صاحب دور أساسي، في إدارة واستثمار البنية التحتية لهذا الفضاء، بما فيها من اجهزة، وخوادم، وتطبيقات، وبرامج، ووسائل اتصال، وطاقات بشرية، وخبرات، تجعل حفظ البيانات، والمعلومات، ومعالجتها، وتبادلها، ممكنا.

ويشهد هذا الفضاء توسعا وانتشارا غير مسبوقين، يستدعيان بذل جهود خاصة، لإقرار سياسات واستراتيجيات عسكرية، تضمن أمن المجتمع والدولة، من جهة أولى، ولوضع الاطر التنظيمية والتشريعية، التي تضمن عدم الاعتداء على الحريات والحقوق، من جهة ثانية.

ويطاول التعاون، المستوى الداخلي، كما يطاول المستوى الخارجي. ففي الجانب التقني، وعلى المستوى الداخلي، شدد نائب وزير الدفاع الأميركي، في خطابه حول الاستراتيجية الدفاعية، أمام الكونغرس، على أهمية التعاون، مع القطاع الصناعي العسكري، وقطاع تكنولوجيا المعلومات والاتصالات، بما يسمح بإيجاد حلول تقنية، لمواجهة الأخطار بشكل فاعل. بينما تتعاون الولايات المتحدة، وغيرها من الدول، في إطار اتفاقيات ثنائية، كما في إطار الناتو، على وضع سياسات واستراتيجيات، في مواجهة الأخطار السيبرانية.

فالتعاون مطلوب لاسباب عديدة، ليس أقلها، طبيعة الشبكة العالمية للمعلومات، التي تتخطى الحدود الوطنية، وتربط الدول بعضها ببعض، والبنى التحتية، والمصالح الحيوية، من جهة أولى، وحداثة الفضاء السيبراني، الذي يتطور بسرعة هائلة، منعت اللحاق به، تشريعيا وتنظيميا، بصورة ملائمة حتى الآن، من جهة ثانية.

ولعل ما يجب ان يحث العرب، على الالتفات بجدية قصوى، إلى ضرورة الحفاظ على أمنهم السيبراني، هو ما قاله موسكوفيتش المسؤول العسكري الاسرائيلي، في حديثه عن المفهوم الجديد لحرب المخابرات، وعن رؤية اسرائيل للحرب المستقبلية، حيث اعتبر ان المعلومات أساس في ربح المعركة، وانه يكفي ان تجمع المعلومات، على نطاق واسع، ومن مصادر مختلفة، ليعاد ارسالها إلى الوحدات المقاتلة. أما مقومات نجاح العملية، فهي بحسب موسكوفيتش، نظام تحكم عن بعد بالبنية التحتية، أنظمة معلومات، والقدرة على دمج المعلومات، واستخراج الملائم منها [148]. ففي الحرب المقبلة، مع لبنان مثلا، توقع ان تتم قيادة القوات المسلحة، وتوجيهها، من خلال مراكز مجهزة بشاشات، وأنظمة معلومات.

وبالفعل، فقد دخلت التدريبات على عمليات سيبرانية، في صلب المناورات العسكرية، الدفاعية منها والهجومية. فقد كشفت صحيفة «يدعوت أحرونوت» ، مؤخرا، أن الجيش الاسرائيلي، يعد لعمليات هجومية، تهدف إلى تدمير مفاعلات نووية عن بعد[149]، عبر التحكم بأنظمة تبريد المياه. إضافة إلى ذلك، تلحظ تدريبات الهجمات السيبرانية، التحكم بحركة النقل البري، والجوي، وموارد الطاقة،

---

[148] *What Israel’s Next War Will Look Like Moscovitch says. “You need a teleprocessing infrastructure, information systems, the ability to integrate and filter information.” - http://www.haaretz.com/israel-news/.premium-1.716800*

[149] العدو يعّد لعمليات هجوم على رأسها تدمير مفاعلات نووية عن بعد - *http://www.al-akhbar.com/node/238381*

وأنظمة إطلاق الصواريخ المضادة للطائرات، بهدف تعميم الفوضى، وايقاع الضحايا بين المدنيين. إلى جانب ذلك، تنظم اسرائيل العديد من الدورات التدريبية على التنصت، ومراقبة الاتصالات.

الا أن اسرائيل، التي تعتبر في قائمة لائحة الدول الأكثر تطورا في مجال الأمن السيبراني، تعرضت أنظمتها لعدد من الاختراقات، من هاكرز في لبنان، وإيران، والسعودية.

٩. منزلقات المواجهة والرد

تضطلع القوى الأمنية بمهمة حماية الأمن القومي، بكل أبعاده، بناء على اطر قانونية وتنظيمية، وطنية ودولية، تحدد الأولى صلاحياتها، ومجال عملها، وتراتبية واصول اتخاذ القرارات، الخاصة بممارسته لدوره الوطني، بينما تحدد الثانية، شرعية الأعمال الحربية أو الدفاعية، في مواجهة البلدان الاخرى. ويتم الامر الأخير، انطلاقا من المعاهدات والاتفاقات الدولية، التي تلتزم بها السلطات السياسية المعنية، تجاه المجتمع الدولي.

الا ان هذه القواعد والاطر التقليدية، لا يمكن الركون اليها، في مجال الاضطلاع بمهمات الدفاع والحماية، والهجوم، في الفضاء السيبراني، كونها أقرت قبل ظهوره. وعليه، ما زالت الحرب السيبرانية، خارج هذه القواعد، وتعتبر القواعد الخاصة بها، مثيرة للجدل، باعتبارها تطاول مجالا حديثا. هذا، عدا عن انها تهيئ ارضية خصبة، للتعرض للحريات والحقوق المدنية، من قبل السلطات الأمنية.

وعلى سبيل المثال، فقد استخدمت الإدارة الأميركية، بعد الحادي عشر من سبتمبر ٢٠٠١، مبرر "مكافحة الإرهاب"، كذريعة لاستخدامها تقنيات حديثة للرقابة، على مواقع الانترنت، والاتصالات الهاتفية، وتصميم برامج إلكترونية للتجسس. ويجري العمل، في بعض البلدان الأوروبية، وفي طليعتها المانيا، على تصميم فيروسات مشابهة لتلك التي يستخدمها القراصنة والإرهابيون، يمكنها اختراق أجهزة الحاسوب والاتصال، الخاصة بهم، لمساعدة الأجهزة المعنية، على رصد الهجمات.

الا أن هذا الامر يشكل، بحسب العديد من الهيئات التشريعية، والخبراء القانونيين، انتهاكًا للحقوق والحريات المدنية. ولعل أبرز المخاوف، تلك المتعلقة بانتهاك الحق في الخصوصية، نتيجة استخدام تقنيات الرصد والتنصت والمراقبة وجمع المعلومات، لاسيما منها تلك الحساسة.

وقد أثارت فضيحة التجسس، التي تقوم بها الولايات المتحدة الأميركية، مخاوفا أكثر جدية، على سلامة العلاقات بين الدول، وعلى الحقوق والحريات الشخصية[150]. فماذا لو قررت إحدى الدول الرد على هذه الاعتداءات الأميركية، باعتبارها اعتداء على أمن المواطنين لديها، والأمن القومي؟ وماذا لو سبب الرد بأضرار مادية رتبت خسائر بشرية، نتيجة انطلاق أسلحة، أو مواد سامة، أو نتيجة اضطراب أو توقف شبكات حيوية، كالنقل، والصحة، والطاقة؟

ويبقى الأخطر، غياب تعريف متفق عليه، لما يمكن اعتباره حربا سيبرانية، يقر للدولة المستهدفة، الحق في الرد. فقد نشرت فرانس ٢٤ خبرا، عن اقتحامات أنظمة معلومات، لشركات تتولى إدارة موارد

[150] *NSA Prism surveillance scandal downplayed by UK government - William Hague denies GCHQ tried to bypass privacy laws, as classified papers show Britain had access to Prism since 2010. http://www.guardian.co.uk/world/2013/jun/09/nsa-prism-uk-government*

الطاقة في أميركا، من قبل قراصنة ايرانيين، استهدفت جمع معلومات، بهدف توجيه ضربة إلى هذا القطاع، بحسب الأميركيين[151].

الا أن الحرص على الخصوصية، والحاجة إلى الحفاظ على الأمن القومي، ومكافحة الإرهاب، لا يجب ان تتحول إلى حجة، لإقرار قوانين تمنع النفاذ إلى الشبكة العالمية للمعلومات، لاسيما وان هذه الأخيرة، قد اثبتت دورها، خلال ما اطلق عليه مسمى «الربيع العربي» في حشد ودعم الجهود، للدفاع عن الحقوق الإنسانية[152]، ومناهضة الظلم، والأنظمة الديكتاتورية.

لهذه الأسباب، تجهد بعض الدول، لإقرار قوانين تسمح لها بالتجسس على الإنترنت، بموجب إذن قضائي.

فقد اقرت مجموعة من المتخصصين، في دراسة حول القانون الواجب التطبيق، على الحرب السيبرانية، وضعت بناء على طلب مركز الدفاع السيبراني، التابع للناتو، بحق الدول في الرد، بطريقة تتناسب وأهمية الاضرار، التي الحقها الهجوم السيبراني، بمصالحها[153]. واستندت الدراسة إلى القانون الدولي، لاسيما منه قاعدة jus ad bellum، التي تبرر الأعمال العسكرية، ضد بلد آخر، وقاعدة jus in bello، التي تحكم التصرف، في النزاعات العسكرية.

وفي الرابع من شهر نيسان (ابريل) ٢٠١٣، نشرت صحيفة أميركا اليوم[154]، خبرا عن وضع البنتاغون للمسات الأخيرة، على قواعد تعطي القيادة العسكرية، صلاحيات واضحة، للرد على الهجمات السيبرانية.

ويثير هذا الواقع، أسئلة كثيرة، ليس أقلها: ماذا عن استهداف الأعمال الجرمية، والاعتداءات، للبنية التحتية وتدميرها أو تعطيلها؟ ومتى يمكن اعتبار هذه الأعمال حربية؟ وهل يؤثر في ذلك، كون المعتدي فردا أو دولة؟ وماذا لو كان الفرد، مقيما في الدولة التي انطلق منها الاعتداء، ولا يحمل جنسيتها؟ وكيف يحدد المدى الجغرافي للرد؟ وماذا عن حقوق الأفراد والمواطنين؟ وكيف تؤمن حماية المدنيين؟

[151] *La cybermenace iranienne donne des sueurs froides à Washington- Dernière modification : 24/05/2013 - http://www.france24.com/fr/20130524-iran-cyberattaque-piratage-hacker-energie-amerique-menace-banque-informatique-internet*
- Iran Hacks Energy Firms, U.S. Says Oil-and-Gas, Power Companies' Control Systems Believed to Be Infiltrated; Fear of Sabotage Potential- http://online.wsj.com/article/SB10001424127887323336104578501601108021968.html

[152] وبالنظر إلى أن الإنترنت أصبحت أداة لاغنى عنها لتحقيق عدد من مبادئ حقوق الإنسان، ومكافحة عدم المساواة، وتسريع التنمية والتقدم الإنساني، ينبغي ضمان حصول الجميع على خدمة شبكة الإنترنت وأن يكون من أولويات جميع الدول

[153] *The Tallinn Manual on the International Law applicable to Cyber Warfare commissioned by NATO- http://www.google.com.lb/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=2&ved=0CDIQFjAB&url=http%3A%2F%2Fwww.nowandfutures.com%2Flarge%2FTallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf&ei=CFKgUe_nDeTA7Aaa4IGAAw&usg=AFQjCNEXPidhfqVoJCLjyQksHEChc1CC3Q&sig2=ne5xXDgk6IzEee1Hfd2sgw&bvm=bv.47008514,d.bGE*

[154] *Jim Michaels5:47 p.m. EDT April 4, 2013-http://www.usatoday.com/story/news/nation/2013/04/04/pentagon-wants-cyber-war-rules-of-engagement/2054055/*

١٠. الصلاحيات والمسؤوليات

مقابل التوسع التقني، والتطور الهائل، ازدادت التحديات القانونية الناتجة عن استخدام وسائل الاتصالات والمعلومات، وبرزت حقوق جديدة، كالحق في النفاذ إلى الشبكة[155]، والحق في الوصول إلى المعلومات، واقرت موجبات على الدولة، لناحية ضرورة تسخير التقنيات في النمو والتنمية، وإيجاد الاطر التشريعية والتنظيمية المناسبة، لتعزيز الثقة في الفضاء السيبراني، وتعميم ثقافة الأمن السيبراني. هذا، إلى جانب ما أفرزته الجرائم السيبرانية، وأخطار الحرب السيبرانية، من تحديات، تستدعي إيجاد أطر تحديد للمسؤوليات، ولقواعد ردع الاعتداءات والجرائم، وإنزال العقوبات الخاصة بها، في حال حدوثها.

ويظهر هذا الامر جليا، في غياب تعريفات قانونية واضحة، ومتفق عليها، للأعمال الجرمية السيبرانية، والأعمال السيبرانية الحربية. يضاف إلى ذلك، ما يتركه من آثار، على مستوى تحديد الصلاحيات القانونية، والحق في المتابعة، والقدرة على جمع الأدلة، بطريقة موثوقة، والقوة الثبوتية للأدلة، والقيمة القانونية للإجراءات الاحتياطية والتنفيذية.

فبالرغم من غموض مفهوم الحرب السيبرانية، الا انه بالامكان اعتبارها، عملية استخدام تقنيات المعلومات والاتصالات، في سياق نزاع مسلح، أو تحضيراً له، كما حصل في الحرب الروسية على جورجيا في العام ٢٠٠٨، عندما هوجمت جميع المواقع الحكومية، وتعطلت الاتصالات، وشلت بين مختلف اجهزة الدولة، والمواطنين. الا ان الحرب السيبرانية بالتأكيد، تختلف، أقله من حيث أسبابها، وهدفها، عن عمليات التسلل الى الانظمة، لجمع بيانات أو تصديرها أو إتلافها أو تغييرها أو تشفيرها، وعن عمليات السيطرة على الانظمة، وتبديلها أو التلاعب بها.

وغني عن القول، ان العالم قد عرف نوعا من هذه الصعوبات، مع المجالات الاخرى، كالمجالين الجوي والبحري، واستخدام الفضاء، أي في المجالات، التي تفرض طبيعة النشاطات فيها تجاوز الحدود، والاتفاق على إدارة المسائل، التي تقوم على إيجاد التوازن بين ضرورات التنمية، ومبدأ احترام سيادة الدول، والحفاظ على سرية ما تراه ضروريا لأمنها، من مواقع ومناطق لديها. كما تعمل الدول مجتمعة، على تنظيم العديد من المسائل ذات الانعكاسات القانونية، في زمن الحروب، كضرورة تحييد المدنيين، واحترام مبدا الرد المناسب لحجم الاعتداءات، وعدم الاعتداء على حقوق الإنسان، وغيرها، الامر الذي يستدعي مسؤولية الدول عن عدم الالتزام بذلك. هذا، ويفترض بكل دولة، ان تؤمن الاطر التشريعية اللازمة، التي تضمن عدم تحولها إلى جنات للجريمة، في المسائل التي يمكن ان تؤثر على الاستقرار والسلم الدوليين، مثل حال الجرائم العابرة للحدود، سواء منها الاقتصادية، كغسل الأموال، والاتجار بالمواد الممنوعة والأسلحة، أو الإنسانية كالاتجار بالرقيق، والأعضاء البشرية.

وإذا كان واقع الحال، يؤكد على ضرورة التعاون الدولي، الا أن الاتفاقات الدولية، في هذا المجال، ما زالت في بداياتها، بالرغم من الحاجة الماسة إلى الاسراع في تطويرها، والانضمام إليها، بما يضمن ليس سلامة الإنسان والمجتمع فقط، بل وبما يضمن حقوق الدول، وسيادتها، والاستقرار والسلم الدوليين.

[155] فقد اعتبر تقرير صادر عن الأمم المتحدة في ٣ حزيران/يونيو ٢٠١١، أن الحصول على خدمة الإنترنت حق من حقوق الإنسان الأساسية

١١. خطوات لا بد منها

بهدف الدفاع الفاعل عن الأمن القومي، تحتاج الجيوش، إلى نقلة نوعية، ترتبط بالسعي الجاد إلى الإفادة من تقنيات المعلومات والاتصالات، ومنع حصول فجوة تؤدي إلى تسرب المخاطر منها. كما ينبغي الاهتمام، بإعداد الكفاءات العلمية والتقنية الوطنية، وحشد الجهود، في إطار خطة تستهدف مواكبة التطورات التقنيات الحاصلة، في مجال الشؤون العسكرية. هذا عدا، عن ضرورة إيجاد الاطر التشريعية والتنظيمية المناسبة، وتخصيص الموارد المالية الكافية لأعمال البحث، والتأهيل، والتدريب، والتطوير في المجال العسكري، والتعاون مع مراكز الابحاث، والجامعات، والقطاع الخاص، لتعزيز القوى الأمنية، وتحقيق التعاون فيما بينها، في جميع المجالات التقنية والقانونية.

أما الخطوة الضرورية في المدى القريب، فيمكن أن تكون إنشاء غرفة عمليات متخصصة، في مراقبة الهجمات السيبرانية، التي تتعرض لها أنظمة معلومات المؤسسات الحساسة، كتلك الخاصة بالدفاع والجيش، والمؤسسات الأمنية، من قبل كادرات قادرة على احباطها، والحد من آثارها. ومن الافضل، أن تعمل هذه الغرفة، بوتيرة تتناسب مع نبض الفضاء السيبراني، أي على مدار ٢٤ ساعة يوميا، كي تتمكن من السهر، على تأمين الحماية اللازمة، لهذه الأنظمة.

قياسا على ما تقدم، وعلى التوصيات الصادرة، عن مختلف الهيئات الدولية المتخصصة[156]، بشكل عام، وعن الاتحاد الدولي للاتصالات، وخطته «لتعزيز الأمن السيبراني العالمي»، بشكل خاص، واستنادا إلى حقيقة ان الموازنة العسكرية، هي الوسيلة التي تسمح بتنفيذ الاستراتيجيات، والسياسات الوطنية في مجال الدفاع، بات لزاما، ان تتضمن بنودا خاصة، بالامور التالية:

- التجهيزات الالكترونية المتطورة، سواء أكانت اجهزة أو برامج، أو منصات، أو تطبيقات، لاسيما منها، تلك التي تضمن حماية الانظمة والمعلومات.
- تدريب محققين وضباط، لجمع الادلة الرقمية وتحليلها، ومواكبة المستجدات، والتعاون مع الاجهزة المماثلة.
- إيجاد آليات تعاون مع القطاع الخاص، حيث الكفاءات العالية، وتسخيره كخط دفاع أول، لضمان حماية الانظمة والمعلومات، والعمليات العسكرية.
- وضع آلية للمراقبة، والإنذار، والرد المبكر، مع ضمان قيام التنسيق عبر الحدود.
- بناء القدرات البشرية، والمؤسساتية، لتعزيز المعرفة وللتمكين، في جميع المجالات المعلوماتية.
- التقييم المستمر لبرامج الحماية، والمكافحة والآليات القانونية المتبعة.
- اعتماد تقنيات التشفير، في حفظ الملفات العسكرية كافة.

[156] مجموعة الدول الثماني، الاتحاد الدولي للاتصالات، الهيئة العامة للأمم المتحدة، مجلس أوروبا والاتحاد الاوروبي

الفصل السادس
الإرهاب السيبراني

يشكل الإرهاب السيبراني، نوعا من أنواع النزاعات السيبرانية. وسنستند في مقاربته، إلى المبدأ القائل، بان انتقال النشاطات الإنسانية إلى الفضاء السيبراني، حمل معه مشاكل وتعقيدات هذه النشاطات، الشرعية منها وغير الشرعية، ومن مبدأ، ان ما هو غير شرعي في الحياة المادية، وفي المجتمع التقليدي، خارج تقنيات المعلومات والاتصالات، يبقى غير شرعي، على الانترنت وفي الفضاء السيبراني. ولا بد لنا من التوقف، عند مدلول الإرهاب في العالم المادي، قبل الانتقال إلى الإرهاب الإلكتروني. مع ملاحظة، ان الهدف ليس دراسة معمقة، ولا تحليلا لتعريفات الإرهاب ووسائله، وانما تأطيرا للإرهاب الإلكتروني، ومحاولة توضيح للمسائل المحيطة به. لذلك، نبدأ من تعريف الإرهاب.

١ . تباين في المفاهيم

عرف ابن خلدون الإرهاب في مقدمته على انه: "القهر والبطش بالعقوبات والتنكيل، والكشف عن عورات الناس". وعليه، فقد رافقت هذه الأعمال، المجتمعات البشرية، منذ ظهورها، وترجمت عمليا، من خلال لجوء فرد معين أو جماعة، إلى بث الخوف والرعب، لدى أفراد أو جماعات اخرى، سعيا لتحقيق أهداف معينة، غالبا ما تمحورت حول نهب وسلب المقتنيات المادية، والاراضي، والمحاصيل. لكن ممارسته، كوسيلة لاسترداد حق، أو أرض، أو ممتلكات وسلطة، اوجدت اختلافا حول النظرة اليه، وحول شرعية الأعمال التي يمثلها. والى هنا ترجع الكثير من الخلافات حول تعريفه. وعلى سبيل المثال لا الحصر، تطرح مسألة توصيف اعمال بث الرعب، واثارة البلبلة، والتفجير، والقتل، التي يمارسها المقاومون في مواجهة الاحتلال.

وهنا أيضا، تدخل اعتبارات كثيرة، ليس أقلها السياسية منها. فما اعتبر مقاومة فرنسية في مواجهة الاحتلال الالماني، لا نراه يطبق على المقاومة الفلسطينية، في مواجهة الاحتلال الاسرائيلي. كما اعتبرت الأعمال الإرهابية، التي مورست من قبل الشيوعيين الماركسيين، في روسيا، ضد القيصر وعائلته والطبقة الحاكمة، ثورة مجيدة، بينما صرح لينين نفسه، عبر اعدامه أفراد الجيش الابيض دون محاكمة، ان الأمن الداخلي، لا يقوم إلا بنشر الذعر والهلع، بين اعداء الثورة.

في المقابل، يعتبر التمرد على أوامر الحاكم في بلدان اخرى، تمردا وعصيانا، أو خيانة وطنية، يستدعيان العقاب. والامثلة هنا، ليست للدخول في تحليل وشرح الاسباب الكامنة وراء ذلك، والمبررات أو المسائل الاخرى المتصلة، وانما فقط للإشارة إلى ارتباط الاختلاف بجذور ثقافية، وسياسية، وفكرية.

فبعيدا عن الانترنت، والفضاء السيبراني، يقوم الإرهاب على أفعال مادية، تنفذ من قبل أشخاص، وتطاول أشخاصا آخرين، أو مصالحهم، وأموالهم وسلامتهم الشخصية أو النفسية، كما تطاول الدول

ومصالحها السياسية، والاقتصادية، ومواردها، ومنشآتها، وغير ذلك. وقد عرفت الاتفاقية الدولية لمكافحة الإرهاب، الصادرة في جنيف عام ١٩٣٧[157]، الإرهاب بأنه: «الأفعال الإجرامية الموجهة ضد إحدى الدول، والتي يكون هدفها، أو من شأنها إثارة الفزع أو الرعب لدى شخصيات معينة، أو جماعات من الناس، أو لدى العامة» [158]. الا ان هذه الاتفاقية، لم تدخل حيز التنفيذ، إلى يومنا هذا، نتيجة الخلاف على مدلول هذا التعريف، حيث اعتبره البعض غير واضح، بينما اعتبر البعض الآخر، ان هدف العمليات الإرهابية، ليس اثارة الرعب، بل ان الرعب هو وسيلة لتنفيذ أعمال ذات أهداف سياسية.

في كل الاحوال، لم تتمكن دول العالم، حتى اليوم، من وضع تعريف موحد للإرهاب. فالى تعريف الإرهاب على انه «عمليات يرتكبها الأفراد أو المجموعات» تصر بعض الدول، على إضافة «إرهاب الدولة». وقد اكتفى البعض، بتحديد بعض عناصره[159] ، على ما تشير اليه عدد من الوثائق الدولية، مثل اتفاقية قمع الإرهاب، الصادرة عن المجلس الأوروبي في ١٠ تشرين الثاني، نوفمبر، ١٩٧٦، واتفاقيتين صادرتين عن الأمم المتحدة، الأولى حول اختطاف رهائن في ١٧ كانون الأول، ديسمبر ١٩٧٩، والثانية حول قمع الاعتداءات بمواد متفجرة في ١٥ كانون الأول، ديسمبر، ١٩٩٧.

على خط موازٍ، تعددت التعريفات، التي اعتمدتها بعض الدول، في سياق علاقاتها بين بعضها البعض، وفي إطار المجموعات التي تنتمي اليها.

فقد عمد الاتحاد الأوروبي، مثلا، إلى تصنيف أعمال الجناح العسكري، في «حزب الله»، بالإرهابية، بينما منع هذا التصنيف عن الأعمال الصادرة عن «الجناح السياسي»، فيه[160]. وبغض النظر عن المواقف الشخصية من هذا الامر، لا بد من ملاحظة اللبس الذي يؤدي اليه هذا التصنيف، كما محاولة الايحاء، بان هنالك تمييزا بين جناحين، يخضعان لنفس القرار، والى اعمال تنفذ بتعليمات وأوامر صادرة، عن نفس الجهة.

من جهتها، اصدرت الولايات المتحدة الأميركية، قانونا اعتبرت بموجبه «حزب الله منظمة إرهابية»، كما اعتمد «مجلس التعاون الخليجي[161]»، هذا التوصيف أيضا.

وتؤشر قرارات الاتحاد الأوروبي، والولايات المتحدة، كما دول الخليج، إلى معوقات التوصل إلى نص موحد على المستوى الدولي، نتيجة ارتباط هذا التصنيف، أحيانا كثيرة، بمصالح الدول، وليس بصالح المجتمع الدولي ككل.

على المستوى العملي، تطبق بعض القرارات والقوانين في إطار فردي ومحدود. فالتصنيف يطاول أحيانا

---

[157] *http://adala.justice.gov.ma/production/Conventions/ar/Conv_Arabe/CA_Lutte_contre_terrorisme.htm*

[158] *« faits criminels dirigés contre un État et dont le but ou la nature est de provoquer la terreur chez des personnalités déterminées, des groupes de personnes ou dans le public ». - http://legal.un.org/avl/pdf/ls/RM/LoN_Convention_on_Terrorism.pdf*

[159] *la convention du Conseil de l›Europe du 10 novembre 1976 pour la répression du terrorisme*
- la convention des Nations Unies du 17 décembre 1979 sur la prise d›otages
- la convention des Nations Unies du 15 décembre 1997 sur la répression des attentats terroristes à l›explosif

[160] *The US, Canada and Australia have also listed Hezbollah as a «terrorist» group. The EU has blacklisted its military wing. http://www.aljazeera.com/news/2016/03/gcc-declares-lebanon-hezbollah-terrorist-group-160302090712744.html*

[161] *GCC declares Lebanon›s Hezbollah a ‹terrorist› group - Gulf countries announce the decision amid an ongoing row with the Lebanese group over involvement in regional conflicts. - http://www.aljazeera.com/news/2016/03/gcc-declares-lebanon-hezbollah-terrorist-group-160302090712744.html*

مجموعة من الأفراد، وليس دولة. وقد أكدت دول الخليج على سبيل المثال، كما الإدارة الأميركية، ان مفاعيل القرار، كما القانون، تعني بعض الأفراد المتعاطفين أو المنتمين إلى هذا الحزب، ولا تعني العلاقات مع الدولة اللبنانية.

لقد أطلقت احداث أيلول الإرهابية، ضد مركزي التجارة الدولية، في مدينة نيويورك الأميركية، ديناميكية جديدة في محاربة «الإرهاب الدولي. وتتحرك هذه الدينامية، في إطار نظام يقوم على احكام ملزمة في القانون الدولي، ويتكون من بعض الاتفاقيات الدولية السارية المفعول [162]، وبعض القرارات الدولية الملزمة، إضافة إلى قوانين وضعية واتفاقات ثنائية، أو إقليمية، بين الدول. وتقر الأولى هذه المكافحة، في مجالات مختلفة، مثل: النقل الجوي والبري والمجال المالي. وتندرج في هذا السياق، أعمال القرصنة، وخطف الطائرات، والتفجيرات الإرهابية، وتمويل الإرهاب. بينما تستند الثانية، إلى شرعية والزامية القرارات الصادرة عن الأمم المتحدة، بالنسبة لجميع الدول الأعضاء، لاسيما وأنها تصدر استنادا إلى الفصل السابع من الميثاق.

ولعل القرار ٢٢٤٩، الصادر في ٢٠ تشرين الثاني (نوفمبر) من العام ٢٠١٥، هو المثال على القرارات الدولية، التي تتخذ في هذا المجال. فقد استند هذا القرار، في ضرورة اتخاذ الإجراءات اللازمة لمنع وقمع الأعمال الإرهابية، التي ترتكبها داعش، والنصرة، والقاعدة، إلى الفصل السابع.

وبالعودة إلى التعريفات، اعتبر مجمع البحوث العلمية في الأزهر[163]، الإرهاب، بأنه: ترويع الأمنين، وتدمير مصالحهم، ومقومات حياتهم، والاعتداء على أموالهم، واعراضهم وحرياتهم، وكرامتهم الإنسانية، بغيا وافسادا في الأرض.

أما مجمع الفقه الإسلامي، التابع لرابطة العالم الإسلامي فذهب في تعريفه الإرهاب إلى أنه : «العدوان الذي يمارسه أفراد، أو جماعات، أو دول، بغياً على الإنسان (دينه، ودمه، وعقله، وماله، وعرضه)، ويشمل صنوف التخويف، والأذى، والتهديد، والقتل بغير حق، وما يتصل بصور الحرابة، وإخافة السبيل، وقطع الطريق، وكل فعل من أفعال العنف، أو التهديد، يقع تنفيذاً لمشروع إجرامي، فردي، أو جماعي، يهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم، أو تعريض حياتهم، أوحريتهم، أو أمنهم، أو أحوالهم، للخطر، ومن صنوفه : إلحاق الضرر بالبيئة، أو بأحد المرافق، والأملاك العامة، أو الخاصة، أو تعريض أحد الموارد الوطنية، أو الطبيعية، للخطر، فكل هذا من صور الفساد في الأرض، التي نهى الله سبحانه وتعالى المسلمين عنها في قوله (ولا تبغ الفساد في الأرض إن الله لا يحب المفسدين)[164].

بدورها، عرفت الاتفاقية العربية لمكافحة الإرهاب، على انه: «كل فعل من أفعال العنف، أو التهديد به، أياً كانت دوافعه، أو أغراضه، يقع تنفيذاً لمشروع إجرامي، فردي أو جماعي، ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم، أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر، أو إلحاق

[162] تفاقية طوكيو والخاصة بالجرائم والأفعال التي ترتكب على متن الطائرات والموقعة بتاريخ ١٩٦٣/٠٩/١٤ م
- اتفاقية لاهاي بشأن مكافحة الاستيلاء غير المشروع على الطائرات والموقعة بتاريخ ١٦ /١٩٧٠/١٢م
- اتفاقية مونتريال الخاصة بقمع الأعمال غير المشروعة الموجهة ضد سلامة الطيران المدني والموقعة في ١٩٧١/٠٩/٢٣م، والبرتوكول الملحق بها والموقع في مونتريال ١٩٨٤/٠٥/١٠
- اتفاقية نيويورك الخاصة بمنع ومعاقبة الجرائم المرتكبة ضد الأشخاص المشمولين بالحماية الدولية بمن فيهم الممثلون الدبلوماسيون والموقعة في ١٩٧٣/١٢/١٤م
- اتفاقية اختطاف واحتجاز الرهائن والموقعة في ١٩٧٩/١٢/١٧م
- اتفاقية الأمم المتحدة لقانون البحار لسنة ١٩٨٣م, ما تعلق منها بالقرصنة البحرية

[163] *http://www.saaid.net/Doat/adel/8.htm?print_it=1*

[164] القصص/ ٧٧

الضرر بالبيئة، أو بأحد المرافق أو الاملاك العامة أو الخاصة، أو احتلالها، أو الاستيلاء عليها، أو تعريض الموارد الوطنية للخطر».

وقد أصدر عدد من الدول العربية، قوانين خاصة بمكافحة الإرهاب، نذكر منها، على سبيل المثال:

- مرسوم صادر في سلطنة عمان، عرفت الأعمال الإرهابية [165] على انها: «كل فعل من افعال العنف أو التهديد به، يقع تنفيذا لمشروع إجرامي فردي أو جماعي ولغرض إرهابي ، ويكون الغرض إرهابيا إذا كان يهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم، أو تعريض حياتهم أو حرياتهم أو أمنهم أو أعراضهم أو حقوقهم للخطر ، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الاملاك العامة أو الخاصة أو الاستيلاء عليها، أو تعريض أحد الموارد الوطنية للخطر ، أو تهديد الاستقرار أو السلامة الإقليمية للسلطنة، أو وحدتها السياسية، أو سيادتها، أو منع أو عرقلة سلطاتها العامة عن ممارسة أعمالها، أو تعطيل تطبيق أحكام النظام الأساسي للدولة، أو القوانين أو اللوائح».
- أما المشرع اللبناني، فقد عرف الإرهاب في المادة ٣١٤ من قانون العقوبات، على انه: «جميع الأفعال، التي ترمي إلى إيجاد حالة ذعر، وترتكب بوسائل كالادوات المتفجرة، والمواد الملتهبة والمنتجات السامة أو المحرقة، والعوامل الوبائية أو المكروبية، التي من شأنها أن تحدث خطراً عاماً».. علما ان وزير العدل، اللواء اشرف ريفي، كان قد أعد مشروع قانون، لحظ تعريفا أكثر شمولية للإرهاب، وجاء فيه: «خلافاً لأيّ تعريف آخر، يُقصد بالجريمة الإرهابية، أي فعل تخريبي، منظّم أو غير منظّم، صادر عن فرد أو عن مجموعة من الأفراد، بأي وسيلة من الوسائل، بهدف ترهيب المجتمع والمساس بأمنه، أو بالأمن الاقتصادي أو الاجتماعيّ أو السياسيّ للدولة، وتقويض السّلم الأهليّ والوطنيّ»[166].
- ونجد في القانون المصري[167]، في المادة الثانية، من قانون مكافحة الإرهاب، تعريفا للعمل الإرهابي بانه « كل استخدام للقوة أو العنف أو التهديد أو الترويع، في الداخل أو الخارج، بغرض الإخلال بالنظام العام، أو تعريض سلامة المجتمع، أو مصالحه، أو أمنه، للخطر، أو إيذاء الأفراد، أو إلقاء الرعب بينهم، أو تعريض حياتهم، أو حرياتهم، أو حقوقهم العامة، أو الخاصة، أو أمنهم للخطر، أو غيرها من الحريات والحقوق، التي كفلها الدستور والقانون، أو الإضرار بالوحدة الوطنية، أو السلام الاجتماعي، أو الأمن القومي، أو إلحاق الضرر، بالبيئة أو بالموارد الطبيعية، أو بالآثار، أو بالأموال، أو بالمباني، أو بالاملاك العامة، أو الخاصة، أو احتلالها، أو الاستيلاء عليها، أو منع أو عرقلة السلطات العامة، أو الجهات أو الهيئات القضائية، أو مصالح الحكومة أو الوحدات المحلية، أو دور العبادة أو المستشفيات أو مؤسسات ومعاهد العلم، أو البعثات الدبلوماسية والقنصلية، أو المنظمات والهيئات الإقليمية والدولية، في مصر، من القيام بعملها أو ممارستها لكل أو بعض أوجه نشاطها، أو مقاومتها، أو تعطيل تطبيق أي من أحكام الدستور، أو القوانين أو اللوائح».

---

[165] نص المرسوم السلطاني رقم 8/2007 بإصدار قانون مكافحة الإرهاب

[166] مقترح قانون لإنشاء محاكم متخصصة بجرائم الإرهاب في لبنان: وعود لا تجاريها النصوص - *http://legal-agenda.com/article.php?id=1440&lang=ar*

[167] *http://www.aljazeera.net/encyclopedia/events/2015/8/17/%D9%86%D8%B5%D9%82%D8%A7%D9%86%D9%88%D9%86-%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9-%D8%A7%D9%84%D8%A5%D8%B1%D9%87%D8%A7%D8%A8-%D8%A7%D9%84%D9%85%D8%B5%D8%B1%D9%8A*

٢. ظهور المصطلح

يرتبط ظهور مصطلح الإرهاب السيبراني، بظهور الفضاء السيبراني، وتوسع الاعتماد على تقنيات المعلومات والاتصالات، في تنفيذ الشؤون الحياتية اليومية للأفراد، والمؤسسات، والدول.

ويرتبط هذا النوع من الإرهاب، بطبيعة البيئة التي يمارس فيها، ومن خلالها. من هنا، يمكن تعريف الإرهاب السيبراني، انطلاقا من الوسائل التي يمارس بواسطتها، وينفذ من خلالها، أو من خلال الجهة، التي يستهدفها، كذلك. وعليه، يمكن تعريف الإرهاب السيبراني، "بالأعمال التي تستخدم التقنيات الرقمية، والفضاء السيبراني، لاخافة واخضاع الآخرين". كما يمكن ان يعرف، بال: "اعتداءات على أنظمة المعلومات، بدوافع سياسية، أو دينية".

وبحسب التعريف المعطى له، في القانون الأميركي، المنشور على صفحة المكتب الفدرالي للتحقيقات، هنالك تمييز بين الإرهاب الدولي، والإرهاب الوطني. ويقصد بالإرهاب السيبراني، حسب هذا القانون: "كل اعتداء قصدي، ذي دوافع سياسية، على المعلومات، أو النظام المعلوماتي، أو البرامج، أو البيانات، ينتج عنه اعمال عنف ضد مدنيين، سواء ارتكبته مجموعة وطنية، أو عملاء غير مرئيين"[168].

كذلك، أعطى المركز الوطني لحماية البنية التحتية في الولايات المتحدة الأميركية، والذي يشكل جزءا من وزارة الداخلية، تعريفا للإرهاب، على أنه: عمل إجرامي ينفذ من خلال الأجهزة المعلوماتية، ويؤدي إلى عنف، أو موت أو تدمير، ويثير الرعب بهدف اجبار الحكومة، على تغيير سياساتها. من جهته، اعتمد حلف شمال الاطلسي تعريفا[169]، اعتبر الإرهاب، «اي هجوم سيبراني، يستخدم أو يستغل شبكات المعلوماتية أو شبكات الاتصال، لاحداث تدمير كاف لاثارة الرعب، وإرهاب مجتمع، لأهداف إيديولوجية.

وقياساً على ذلك، يمكن القول، أن الإرهاب هو اعمال التدمير، والتلاعب، والتعطيل، وتغيير البيانات، التي تطال حركة تدفق المعلومات، على الشبكة، أو أنظمة المعلومات التي تدير مصالح الدولة الحيوية، أو المصالح الحرجة، والتي تعتبر أساسية لإدارة شؤونها، وسير العمل فيها، بصورة قصدية، وبنية الحاق الاذى، على اوسع نطاق ممكن، لاسباب إيديولوجية، اجتماعية أو سياسية، أو دينية. كذلك، تعتبر التهديدات، بممارسة اي من هذه الأعمال، بهدف الابتزاز أو الضغط، تحقيقا لأهداف سياسية، اعمالا إرهابية، كما يكتفى بالنسبة لنتائجه، ان تحدث ترويعا ورعبا، لدى الأشخاص.

[168] *18 U.S.C. § 2331 defines «international terrorism» and «domestic terrorism» for purposes of Chapter 113B of the Code, entitled «Terrorism”: «International terrorism» means activities with the following three characteristics: Involve violent acts or acts dangerous to human life that violate federal or state law; Appear to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and Occur primarily outside the territorial jurisdiction of the U.S., or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum.* «Domestic terrorism» means activities with the following three characteristics: Involve acts dangerous to human life that violate federal or state law; Appear intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination. or kidnapping; and Occur primarily within the territorial jurisdiction of the U.S. 18 U.S.C. § 2332b defines the term «federal crime of terrorism» as an offense that: Is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct; and Is a violation of one of several listed statutes, including § 930(c) (relating to killing or attempted killing during an attack on a federal facility with a dangerous weapon); and § 1114 (relating to killing or attempted killing of officers and employees of the U.S.). * FISA defines «international terrorism» in a nearly identical way, replacing «primarily» outside the U.S. with «totally» outside the U.S. 50 U.S.C. § 1801(c).*

[169] *NATO Glossary of Terms and Definitions, AAP-06 Edition 2012 Version 2. (NATO) defines terrorism as “the unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives.”*

فقد ارتبط الاهتمام بالإرهاب السيبراني، بظهور الاعتداءات والجريمة السيبرانية، والكوارث التي يمكن ان تسببها، في حال استهدافها المصالح الحيوية للدول. فالاعتداءات على الأنظمة التي تدير توزيع الطاقة والمياه، ذات تأثير مباشر وأكيد، على السلامة العامة، حيث يمكنها ان تثير الذعر، وتخلق جوا من الهلع، وتعرض حياة الناس للمخاطر. علما أن السيطرة على موارد الطاقة، ومولدات الطاقة النووية، وشبكات النقل البري، والبحرين والجوي، يمكن أن تكون بحد ذاتها، هدفا للاعمال الإرهابية. فالسيطرة على أنظمة الحكومة الإلكترونية، يمكنها ان تؤدي إلى تعطيل الخدمات، أووقفها، أو تدميرها، والتسبب، إلى خسائر بشرية ومالية. كما يمكن للسيطرة على الانترنت، ووسائل الاتصال، ان يساعد على التلاعب بالرأي العام، ودفعه باتجاه ردات فعل، تعرض الاستقرار، وتؤدي إلى انهيار النظام، عدا عما يمكن ان تتسبب به من خسائر مادية وبشرية، نتيجة انهيار الثقة. ويبقى الادهى، ان تتعطل الخدمات، في مجال الصحة العامة والاسعاف، نتيجة الاعتداءات السيبرانية، فيعجز المواطن عن الاتصال بالأجهزة المتخصصة، كما تعجز الدولة عن تقديم الخدمات.

وهنا، لا بد من التأكيد، على ضرورة التمييز بين النضال السيبراني، الذي يمكنه ان يتشابه في الدوافع، والوسائل مع الإرهاب، ولكن باختلاف القصد والهدف. حيث لا يسعى النضال السيبراني، إلى الحاق الاذى، لا بالدولة ولا بالأفراد، وانما يسعى إلى توعية المجتمع، واستنهاضه للدفاع عن قضية ما، أو للوقوف إلى جانب مطالب اجتماعية. كما يتميز الإرهاب عن الحرب السيبرانية، بتركيزه على أهداف مدنية، بشكل عام.

ويعتبر الإرهاب السيبراني، من أشد الاعتداءات السيبرانية خطورة، على الانترنت. الا ان تعريف الإرهاب السيبراني، لا يمكن استخدامه لوصف جميع الاعتداءات السيبرانية، التي يمكن ان تمس المصالح الحيوية للمواطنين وسلامتهم، وتثير الرعب فيهم، أو تخلق نوعا من عدم الاستقرار. فالاعتداءات السيبرانية، يمكن ان تكون صادرة عن فرد واحد، أو عن مجموعة منظمة من المجرمين، بينما تكون نتائجها كارثية ومشابهة لتلك التي يرتكبها إرهابيون. وعليه، لا يمكن وصف الاعتداء بالإرهابي، الا متى توافرت فيه عناصر محددة، مثل الهدف السياسي، وهوية المعتدي أو المحرض عليه، ونقطة انطلاقه، وغاياته.

يضاف إلى ذلك، انه ليس من المستبعد ان تكون للجريمة السيبرانية، أحيانا، أبعاد كارثية، تؤثر في حياة الناس، وتثير لديهم الذعر أيضا، كأن يتمكن أحد الأفراد، من التحكم بأنظمة معلوماتية متصلة بالبنية التحتية للدولة. فليس غريبا ان يشن الاعتداء على أحد أنظمة توزيع الكهرباء أو المياه، أو حتى الخدمات المصرفية والمالية، والتي تعود ملكيتها كما ادارتها إلى القطاع الخاص، ويكون الهدف جني الارباح، وابتزاز الجهة المالكة لدفع فدية.

ويقودنا ذلك، إلى امكانية التمييز بين الاعتداءات الإرهابية، والجريمة السيبرانية. ويرتكز هذا التمييز إلى أهداف كل منها. فالجريمة تسعى إلى المال والارباح، بينما يهدف الاعتداء الإرهابي، إلى الضغط السياسي، وفرض شروط على السلطة، عبر استعراض قوة يثير الذعر والهلع.

الا ان هذا التمييز يبقى صعبا وغير دقيق، احيانا كثيرة، لاسيما عندما تتشابه النتائج، بين الجريمة السيبرانية، والإرهاب السيبراني، كما أسلفنا. وما يزيد الامر صعوبة، هو الارتباط الممكن بين الجريمة السيبرانية

والإرهاب السيبراني، لاسيما عبر القنوات المالية. فالجريمة السيبرانية، ترى في الإرهاب مصدرا للمال والسلطة، كما يرى الإرهاب في الجريمة، وسيلة لجمع المال وتأمين الموارد. وهكذا يلجأ الإرهابيون، إلى استخدام خبرات المجرمين السيبرانيين وأدوات تنفيذ إرهابهم، مقابل مبالغ من المال. اما المثال الذي يمكن سوقه هنا، فهو شراء البرامج الخبيثة، والروبوتات، لاستخدامها في تنفيذ الاعتداءات على الأنظمة المعلوماتية، وتعطيل الخدمات، واختراق الحسابات، واقفال المواقع الحكومية، وتعطيل مراكز الخدمات العامة، ووسائل الدفاع.

٣. استخدام المجموعات الإرهابية للانترنت

تقدم الانترنت منبرا هاما، يطل الإرهاب من خلاله، سواء لترويع المجتمع، أو لإدارة عملياته التي ينفذها في اماكن مختلفة من العالم، وتأمين الاتصال بين مجموعاته، أو حتى لبث ثقافة، أ وفكر، أو إيديولوجية معينة، والحشد لها. وتتنوع المواقع الإرهابية، كما تتنوع الرسائل، والتهديدات، والمهمات، التي تقوم بها. والوجود الإرهابي على الشبكة العالمية، يستفيد من تقنيات الاخفاء، والمجهولية، كما يستفيد من امكانات وخبرات المجرمين، في مجال تغيير عناوين الانترنت، في الانترنت المظلم، حيث تنتشر أخطر أنواع الجرائم. ويساعد هذا الامر، في ظهور مواقع إرهابية، تؤدي مهمة محددة، لفترة قصيرة، تعود بعدها إلى الاختفاء.

أ– الانترنت المظلم: المجهولية وإخفاء الأثر

فالانترنت المظلم، هو جزء من الانترنت الخفي، الذي لا يمكن الوصول اليه، باستخدام المتصفحات العادية، أو محركات البحث، التي نستخدمها على الشبكة العالمية للمعلومات، مثال غوغل، أو ياهو، أو فاير فوكس. فللانترنت المظلم، متصفحات خاصة، مثل تور TOR[170]، فريبتو Freepto[171]، وفرينت Freenet[172]، وغيرها. اما الميزة الأساسية لهذه المتصفحات، فهي إخفاء الأثر، الذي يمكن ان يتركه المتجول على الانترنت، ومنع تعقبه ومراقبته، ما يتيح له:

- حماية هويته ومعلوماته.
- إنشاء مواقع على الانترنت، دون كشف هويته أو مكان وجوده.
- تجاوز برامج الحجب المعتمدة في بعض البلدان.
- تكوين شبكات تبادل معلومات آمنة، وارسال معلومات سرية.

[170] تور برمجية صممت لزيادة مجهولية المستخدِم على الإنترنت. فهي تُنكّر هوية ونشاط المستخدم لمقاومة أساليب كثيرة من تقنيات مراقبة الإنترنت. وسواء أكانت المَجهولية مهمة لك أم لا، فإن تور يفيد كوسيلة مؤَمّنة لتخطي الرقابة على الإنترنت لتتمكن من مطالعة المواقع ونشر المحتوى - *https://securityinabox.org/ar/tor.*

[171] *Freepto is a Debian based operating system on a USB stick developed by hacktivist group AvANA and used, in between others, by various anarchist groups like the Spanish CNT group in Madrid selling USB thumbdrives with Freepto loaded and hacker spaces in Greece and Italy that do Freepto presentations during digital security training. http://www.hacker10.com/internet-anonymity/encrypted-operating-system-for-activists-freepto/*

[172] *Freenet is free software which lets you anonymously share files, browse and publish «freesites» (web sites accessible only through Freenet) and chat on forums, without fear of censorship. Freenet is decentralised to make it less vulnerable to attack, and if used in «darknet» mode, where users only connect to their friends, is very difficult to detect - https://freenetproject.org/about.html*

ويتم تأمين ذلك، عبر تقنية ترتكز، بشكل أساسي، على تشفير البيانات، وعلى شبكة من الآف المخدمات الموزعة حول العالم، التي تستقبل طلبات الدخول إلى المواقع، وتقوم بترميزها قبل اعادة ارسالها، بحيث توزع المعلومات الخاصة بالهوية، والموقع، ونظام التشغيل، على عدد من المخدمات الوسيطة، بما يؤمن اخفاء هوية المتصفح، وسرية التصفح والحركة، عبر منع عملية الجمع بين عناصر الهوية. وقد بدأ TOR، كمشروع، في مختبر أبحاث تابع للقوات البحرية الأميركية، لتأمين شبكة اتصالات خاصة، تضمن خصوصية وسرية المعلومات، والأجهزة الأمنية المتصلة بها. وكان من الطبيعي، ان يلجأ إلى استخدام هذا المتصفح، أو ما يماثله من متصفحات، الراغبون بالحفاظ على سرية معلوماتهم، وحركتهم على الشبكة، بعيدا عن الرقابة والرصد. ويندرج في هذه اللائحة: العاملون لدى المنظمات الدولية، والهيئات الحكومية، والأجهزة الأمنية، والمدافعون عن حقوق الإنسان، وكل من يحتاج إلى حرية الحركة، ويخاف السلطات القمعية. الا ان الجريمة، لم تتأخر في الافادة من تقنيات الاخفاء، التي تقدمها هذه المتصفحات، لممارسة نشاطها بعيدا عن عيون السلطات، واخفاء آثارها. وبات الانترنت المظلم، مركزا لجميع أنواع الجرائم الخطرة، مثل بيع المخدرات، والأسلحة، وتأمين المرتزقة لجرائم قتل وسرقة، واتجار بالبيانات المسروقة من الانترنت.

لكل ذلك، يصعب القضاء على المواقع الإرهابية، كما على الحسابات الخاصة بالمنظمات الإرهابية، على مواقع التواصل الاجتماعي، حيث تختفي لتعود إلى الظهور، بأسماء وعناوين جديدة.

ب- الشبكة العالمية للمعلومات

بعيدا عن استخدام الانترنت المظلم، يلجأ الإرهابيون إلى الشبكة العالمية للمعلومات، التي يصلها جميع المستخدمين حول العالم، ليس للاتصال بمناصريهم واعوانهم، ممن لا يتواجدون في الانترنت المظلم وحسب، بل للاتصال بالعالم أيضا، وبجميع مستخدمي الانترنت. فعبر الانترنت، يوجه الإرهاب رسائله إلى الإعلام، والى مجتمعات معينة، كما إلى السلطات والحكومات، بهدف نشر الرعب، وبث الذعر، وشن حملات نفسية ضد من يعتبرونه عدوا لهم. وقد وجهت داعش، ومن قبلها القاعدة، العديد من رسائل الترهيب، كما نشرت خطابات زعمائها، وافلاما مرعبة لكيفية تعذيب الاسرى والمعتقلين، والاعدامات وعمليات القتل الوحشية، مقدمة نفسها، كصاحب قضية عادلة.

وكانت القاعدة، قد أنشأت موقعا رسميا لها، بعد احداث الحادي عشر من ايلول، نشرت من خلاله بياناتها الرسمية، كما أنشأت صحيفة إلكترونية، تصدر عن الجهاز الإعلامي لديها، إضافة إلى عدد من النشرات التي اهتمت بالترويج لفكرها، ولفكر قادتها ومنظريها، واخرى خاصة بالمعلومات العسكرية والتجنيد.

وهكذا يستخدم الإرهابي الشبكة، على مستويات عدة، منها:

- بناء المعلومات، عبر التنقيب عن البيانات، فيجمع الاخبار المتعلقة بمكافحة الإرهاب، والمعلومات الخاصة بمواقع المنشآت الحكومية، في البلدان المستهدفة، مثل المطارات، والمنشآت العسكرية، والحكومية، واماكن المنشآت النووية.
- الاتصال والتنسيق مع أفراد ومجموعات المنظمات الإرهابية، وتبادل المعلومات معهم، وتوزيع المهمات، ومتابعة تنفيذ الهجمات الإرهابية، ليس فقط على الانترنت، وانما في العالم المادي أيضا.

فقد استخدم إرهابيو القاعدة الانترنت، بشكل مكثف في تنفيذ اعتداءات أيلول، سبتمبر ٢٠١١، على مركزي التجارة الدولية، في نيويورك.

- تجنيد أشخاص جدد، لمواصلة النشاط الإرهابي، وتعزيز قدراته، وفرص استمراره. وتتم عملية التجنيد، عبر غرف الدردشة، ووسائل التواصل الاجتماعي، أو حتى بواسطة الرسائل المباشرة على الهواتف الذكية. وكانت دراسات حديثة، قد أظهرت لجوء الإرهابيين إلى تجنيد الشباب التونسي[173]، للقتال في سوريا، إلى جانب داعش وجبهة النصرة وغيرها، عبر استهداف شريحة معينة من الشباب، تشكو من مشاكل اجتماعية، واقتصادية، أو نفسية، نتيجة الاوضاع المزرية التي يعيشون فيها ، فتستثمر مهاراتهم العلمية والقتالية. ولعل ما أوضحه أحد المسؤولين، في إطار هذه الدراسة، عن الاسباب الكامنة وراء نجاح الإرهابيين في تجنيد الشباب، مؤشر على المكان الذي يجب ان تبذل الجهود فيه، لمنع هذا التجنيد. فقد برزت من الاسباب، على سبيل المثال: محدودية المستوى العلمي، والبطالة والفقر، وغياب الإطار القانوني المناسب لمكافحة هذه الآفة، وعدم مراقبة المواقع الجهادية، وغياب السياسة الجدية لوقف النزيف. مع الإشارة، إلى ان محدودية المستوى العلمي، يمكن تفسيرها، على مستوى استيعاب القضايا الجهادية، والتعامل مع الفكر التكفيري. ذلك ان الدراسة، قد أبرزت استقطاب هذه الجماعات لطلاب وشباب متفوقين، واصحاب كفاءات علمية عالية.

ولا تبقى البلدان الغربية بعيدة عن مخاطر تجنيد الشباب، على المواقع الإلكترونية، اذ تنشر الصحف والمواقع الإعلامية المختلفة، أخبار تجنيد الشباب في بلدان أوروبا، وأميركا واستراليا. وتتم هذه العملية غالبا، عبر مواقع مخصصة للقتال والقتل [174]. ويعتبر «فيسبوك»، أكثر مواقع وسائل التواصل الاجتماعي استخداماً، في التجنيد، حيث تقوم الجماعات الإرهابية بإنشاء «مجموعات»، لاصطياد من يتوافقون معها فكريا، أو من لديهم استعداد لذلك، موهمة إياهم، بانها تدافع عن قضايا ذات أبعاد دينية وقومية، كالاسلام والقضية الفلسطينية، لتقوم بعد ذلك، بتوفير مواد جهادية، ومن ثم توجيههم إلى مواقع وغرف دردشة، أو منتديات مرتبطة بها مباشرة. ويحذر الخبراء في هذا المجال، من خطر أكيد يكمن في تحول الإرهاب، من الدعاية والتجنيد، إلى شن هجمات سيبرانية، على البنية التحتية، والأنظمة، وسرقة معلومات حساسة، كالخطط، والخرائط، والاستراتيجيات العسكرية.

- توزيع منشورات خاصة، ونشر مواد تعليمية حول كيفية صنع المتفجرات، والقنابل، والأسلحة الفتاكة.
- جمع الأموال والتبرعات، عبر عمليات خداع الأشخاص، والايحاء لهم، بأنهم انما يتبرعون

---

[173] ظاهرة تجنيد الإرهابيين عبر مواقع التواصل الاجتماعي - *http://pss.elbadil.com/2016/03/01/%D8%B8%D8%A7%D9%87%D8%B1%D8%A9%D8%AA%D8%AC%D9%86%D9%8A%D8%AF-%D8%A7%D9%84%D8%A5%D8%B1%D9%87%D8%A7%D8%A8%D9%8A%D9%8A%D9%86-%D8%B9%D8%A8%D8%B1-%D9%85%D9%88%D8%A7%D9%82%D8%B9-%D8%A7%D9%84%D8%AA%D9%88/*

[174] *Now ISIS is using social media to expand its war far beyond its borders. What started with thechoreographed execution video of James Foley, blasted across the Web through an army of dummy Twitter accounts, has now morphed into something more devious and distributed. Rather than calling followers to the front lines, ISIS's social-media strategy cultivates them at home in the U.S., Europe, Africa, and Asia. And it can use those followers to devastating effect, whether sending masked gunmen storming into the Paris Bataclantheater or inspiring an American citizen and his wife to massacre 14 co-workers at a holiday party in San Bernardino, California. TERROR ON TWITTER- How ISIS is taking war to social media—and social media is fighting back. http://www.popsci.com/terror-on-twitter-how-isis-is-taking-war-to-social-media*

لجمعيات إنسانية، واجتماعية، وخيرية، ولقضايا عادلة.

٤. أشكال المواجهة

منذ العام ٢٠١٤، وفي أعقاب الخطة التي أطلقتها الولايات المتحدة الأميركية، تتكثف الجهود الآيلة، إلى ارساء آليات تعاون بين العديد من البلدان، لمواجهة انتشار ظاهرة الدعوات إلى التطرف، عبر الانترنت، لاسيما بعد صعود تنظيم الدولة الاسلامية: داعش.

لم تنقطع الجهود الدولية لمواجهة انتشار التطرف عبر شبكة المعلومات الدولية، ومنظومة الإعلام الجهادي، التي اكتسبت زخماً غير مسبوق عقب صعود تنظيم داعش، وتبنيه لاستراتيجيات الاستقطاب الافتراضي، للمتعاطفين معه. ففي أكتوبر ٢٠١٤، أعلنت الولايات المتحدة عن خطة للتحالف المعلوماتي مع الدول الغربية والعربية، لتنسيق الجهود من أجل مواجهة تنظيم داعش إلكترونيا، عبر مواقع التواصل الاجتماعي.

وفى فبراير ٢٠١٥، خلال قمة مكافحة التطرف والعنف، أكدت الولايات المتحدة الأميركية مرة أخرى، على مخاطر التهديدات الإلكترونية لتنظيم داعش، والذي استطاع في فترة وجيزة، تعزيز قبضته على وسائل التواصل الاجتماعي، وتوظيفها في الترويج لإيديولوجيته، واستقطاب أنصار جدد.

أ- الجهود الفردية

- الولايات المتحدة الأميركية

انطلاقا من ادراكها لخطورة الوضع، عمدت الإدارة الأميركية، في عهد اوباما، إلى اتخاذ التدابير الآتية:

- تعزيز الإطار القانوني والتشريعي، عبر اصدار قانون خاص، لمكافحة الإرهاب على الانترنت [175]، عرف ب «قانون حماية الشبكات السيبرانية».
- تعزيز دور مركز الاتصالات الاستراتيجي لمكافحة الإرهابCSCC، التابع لوزارة الخارجية الأميركية، حيث يعمل عدد من المتخصصين، في تقنيات المعلومات والاتصالات، ويجيدون عددا من اللغات، من بينها العربية. وينشط هذا المركز، عبر توثيق ونشر مواد مناهضة للإرهاب، واعادة نشر ما ينشر من قبل جهات متعاطفة مع حركة مكافحته، سواء أكانت دولا، ام منظمات، أم أفرادا. ويرأس هذا المركز مسلم، يحتل منصب المبعوث الخاص، لمنظمة التعاون الاسلامي[176].
- إطلاق مشروع مخصص للتصدي للحملات الإرهابية، Think again, Turn Away[177] ومحاولات التجنيد على الانترنت، يعتمد على بث تغريدات مضادة للإرهاب، إضافة إلى استهداف حسابات

[175] *The Protecting Cyber Networks Act. Gangs of cyber criminals, sometimes supported by hostile governments, are increasing their attacks on U.S. networks and American businesses. The wave of assaults is a national security threat that is costing our economy billions of dollars and compromising American citizens' personal and financial information. The House Permanent Select Committee on Intelligence is acting to mitigate this growing problem by advancing a bill, the Protecting Cyber Networks Act (H.R. 1560), that will encourage businesses and the federal government to share information on known cyber threats. More information on the bill is available at the links below. http://intelligence.house.gov/ProtectingCyberNetworksAct*

[176] *Appointment of Rashad Hussain as United States Special Envoy and Coordinator for Strategic Counterterrorism Communications. http://www.state.gov/r/pa/prs/ps/2015/02/237585.htm*

[177] *Think Again Turn Away campaign. http://www.latimes.com/nation/nationnow/la-na-nn-state-department-islamic-state-social-001-photo.html*

الجهاديين.

- ارساء قواعد تعاون مع بلدان اخرى، من خلال عدد من المبادرات، مثل: مبادرة التعامل مع الامارات العربية المتحدة، والمملكة البريطانية، سواء من خلال محاربة الإعلام الداعشي، ام من خلال تفعيل التعاون وتبادل المعلومات بين اجهزة طوارئ الانترنت، أو إنشاء خلايا مشتركة، تعمل على رصد التهديدات السيبرانية، وتبادل المعلومات بشأنها.

هذا ويقوم جهاز من المتجسسين في الولايات المتحدة الأميركية، بتمشيط مواقع التواصل الاجتماعي، منقبين في البيانات، التي ينشرها الإرهابيون عن أنفسهم، سعيا إلى توقع خططهم، وتتبع تحركاتهم. وقد نجحوا في العام المنصرم، بتوجيه ضربة جوية إلى احد معاقلهم، نتيجة المعلومات التي تجمعت لديهم، من خلال رصدهم حركة اتصالات أعضاء التنظيم، على وسائل التواصل[178].

ـ أوروبا

بعد الاعتداءات على شارلي ايبدو، شرع الأوروبول في العمل على محاربة داعش، من خلال وحدة خاصة، سميت EU-IRU. وتتولى هذه الوحدة تمشيط الانترنت بحثا عن الحسابات الشخصية، لقياديي الحملات الإعلامية الإرهابية [179]، وتحديد الأشخاص الذين يمكن ان يستهدفوا بغرض التجنيد، إضافة إلى تعقب مصادر تمويل التنظيم.

من جهتها، أنشأت بريطانيا، كتيبة متخصصة في الحرب المعلوماتية، هي الكتيبة ٧٧[180]، تضم خبراء في التواصل الاجتماعي، وتتألف من عناصر في الجيش البريطاني، مهمتهم شن حرب نفسية مضادة، من خلال حسابات انشئت لهذه الغاية، على تويتر وفايسبوك. كذلك، تم إنشاء وحدة متخصصة فرنسية، ترصد حركة تجنيد الفرنسيين، من قبل داعش. كما عمدت الحكومة الفرنسية، إلى اتخاذ قرار بتعزيز قدرات الجيش، خلال السنوات القليلة المقبلة، لمواجهة المخاطر السيبرانية، والإرهاب[181].

ب– دور الهاكرز

لقد انضم بعض الهاكرز إلى حملات المكافحة، فأعلنت مجموعة الهاكرز المجهولين Anonymous، عن نيتها محاربة داعش، وتعقبت مواقعه، حتى زوايا الانترنت المظلم. وقد تمكنت مجموعة منهم، تعمل على رصد مواقع داعش على الانترنت المظلم، من اغلاق مراكز للتجنيد، ولجمع التبرعات من العملة الرقمية، مستبدلة إعلانات داعش، بإعلانات عن مواد تجارية [182]. كذلك، بادر عدد من محركات البحث، والمواقع الاجتماعية، إلى مراجعة سياساتها حول المضمون، في محاولة منها، لمنع المحتوى الذي

---

[178] *Air Force intel uses ISIS ‹moron› post to track fighters. http://edition.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter/*

[179] *On 1 July 2015 Europol launched the European Union Internet Referral Unit (EU IRU) to combat terrorist propaganda and related violent extremist activities on the internet. https://www.europol.europa.eu/content/europol%E2%80%99s-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda*

[180] *British Army›s new 77th Brigade will wage online PSYOP war with terrorists. The British Army has created a new psychological operations and propaganda unit to wage online war and «control the narrative» during conflicts. The 1,500 members of the 77th Brigade will be drawn from across the British Army and Territorial Army reservists, and will begin operations in April. http://www.ibtimes.co.uk/british-armys-new-77th-brigade-will-wage-online-psyop-war-terrorists-1486044*

[181] *Terrorisme : François Hollande annonce la création de 800 nouveaux postes dans l›armée. https://www.francebleu.fr/infos/societe/terrorisme-hollande-annonce-la-creation-de-800-nouveaux-postes-dans-l-armee-1459944646*

[182] *Hackers replace dark web Isis propaganda site with advert for Prozac. http://www.ibtimes.co.uk/hackers-replace-dark-web-isis-propaganda-site-advert-prozac-1530385*

يمجد الإرهاب، ويروج للفكر الإرهابي، والتطرف، والعنف، والكراهية. فعمد يوتيوب، على سبيل المثال، إضافة إلى ازالة المحتوى، إلى ازالة الوصلات غير المباشرة اليه.

وكذلك فعلت مجموعة انونيموس Anonymous، عبر تعقبها عشرات آلاف الحسابات الخاصة بالجهاديين على تويتر، واغلاقها. الا انه، وفي مقابل التقنية التي اعتمدها الهاكرز، من خلال برنامج يتعقب أوتوماتيكيا الحسابات الشبيهة، التي تظهر بعد اغلاق الأولى، عمدت داعش، إلى كتابة برنامج، يخفي أوتوماتيكيا هذه الحسابات عنهم.

كذلك، يلجأ الهاكرز، إلى تقنيات منع الوصول إلى المواقع DDos، فيمطرون مواقع الإرهابيين، بعشرات آلاف طلبات الدخول لتعطيل الوصول اليها، كما يعمدون إلى عرض خدماتهم في اختراق المواقع، وكتابة البرامج المتخصصة لحساب الجريمة، ويعمدون إلى جمع المعلومات، عمن يطلبون هذه الخدمات، مستخدمين تقنيات التحقيق، ورصد الموقع، والهوية، للوصول إلى من يقف وراء طلب خدمات المرتزقة، كما يجمعون معلومات، عن الأشخاص الذين تجندهم داعش، واولئك الذين يتواصلون معها. وقد ساعد هذا الاسلوب، في منع هجوم إرهابي على تونس[183]، وتوقيف عشرات الإرهابيين من مناصري داعش.

وكانت انونيموس، قد أعلنت الحادي عشر من ديسمبر، يوم «مطاردة داعش»[184]، وهو يوم مخصص لحشد المناوئين لهذا التنظيم، في تظاهرة تركز على غبائه الفكري، والسياسي، وعلى رغبة مجتمع الشبكات الاجتماعية، وقوة الارادة في مجابهته. ومن الضروري الإشارة، إلى اهمية تحسيس مستخدمي الانترنت بخطر الإرهاب، وضرورة الانخراط في مواجهته، في البيئة التي تعتبر أكثر خطرا عليه. وبالفعل، فقد تجاوب عدد كبير، مع الدعوات التي اطلقت، حول هاشتاغ داعش #داعش، وتبارى الشباب في نشر الصور والتعليقات[185]، التي تستخف به وتسخر منه.

على مستوى مختلف، يبادر عدد من المواطنين العاديين، المناوئين للفكر التكفيري والداعشي، بتوثيق جرائم داعش، وارتكاباتها الوحشية، ونقلها من خلال مواقعهم على الشبكات الاجتماعية، لاظهار بشاعة هذا التنظيم، وفضح اكاذيبه.

٥. مواجهة صعبة ومقترحات

مما لا شك فيه، ان الخطوة الأولى إلى الشفاء، هي الإقرار بوجود الداء. من هنا، لا بد من وعي خطر الإرهاب السيبراني، والانتباه إلى تداعياته الكارثية، على أمن واستقرار الدول.

---

[183] *BBC Trending - Ghost Security Group: 'Spying' on Islamic State instead of hacking them. The group claims that it has already helped to thwart one attack in Tunisia by picking up on what they say was online jihadi chatter which indicated that militants would attack a specific location on the island of Djerba. The plot, Ghost Security says, was designed to be a follow up to the June beach massacre which killed 38 people, mostly British tourists. Reports indicate that Djerba did indeed appear on a list of IS targets in Tunisia in July. Like the other claims the groups have made, though, it's difficult to verify that they thwarted an attack. http://www.bbc.com/news/blogs-trending-34879990*

[184] *Anonymous declares December 11 ‹Isis Trolling Day. http://www.wired.co.uk/article/anonymous-isis-trolling-day*

[185] *C'est vendredi… le jour J pour se moquer de Daesh. «L'objectif est simple : partager sur les réseaux sociaux, avec le hashtag #Daesh et #Daeshbags, des photos drôles et moqueuses ainsi que des vidéos parodiques de Daesh. « Nous vous demandons de montrer votre soutien et votre aide contre Daesh, en nous rejoignant et en se moquant d'eux. Ne pensez pas que vous devez être membre d'Anonymous : tout le monde peut le faire, cela ne demande pas de compétences particulières » expliquait le groupe sur son compte Twitter». http://www.lesoir.be/1067498/article/soirmag/actu-soirmag/2015-12-11/c-est-vendredi%E2%80%A6-le-jour-j-pour-se-moquer-daesh*

بعدها، يمكن الانتقال إلى وضع استراتيجيات وسياسات تنفيذها، على ان تتقدم خطة توعية شاملة، تأخذ بعين الاعتبار، خصوصية البيئة الحاضنة لها، وفي مقدمها الأيديولوجيات والمعتقدات، التي تحولها إلى جزء من وجدان المجتمع، الذي يتعامل معها، على انها قضيته الخاصة. وهذا يعني، وضع آليات وتدابير احترازية، وصولا إلى إقرار عقوبات جزائية رادعة.

فبرامج المكافحة، كما أشرنا، انطلقت على المستوى العالمي، ومن الممكن الانضمام اليها، والافادة منها، ومن التعاون الذي تتيحه، ومن نقل الخبرات، والإحاطة بتقنيات الرصد، والمتابعة والتنصت، في حدود الحفاظ على حقوق الإنسان والحريات. ولعل الاعتراض، على هذه البرامج، من هذه الزاوية، هو أحد أهم العوائق. حيث تقوم حركات "حماية الحقوق والحريات"، بحملات ضد اجتياح هذه البرامج، للخصوصية والحريات الاخرى، كحرية التعبير والوصول إلى المعلومة. الا ان هذه البرامج، وبالرغم من قدراتها الهائلة، في جمع ترليونات من البيانات، ليست حلا أكيدا، وان كانت تساهم في استشراف المخاطر. ذلك ان برامج التخفي، وبرمجيات تجاوز الرقابة، والانترنت المظلم، ناشطة هي الاخرى.

ففي الصين مثلا، حيث الرقابة الاشمل، الأعمق، ليس فقط للمحتوى، وانما أيضا للوصول إلى التطبيقات والمتصفحات العالمية، والى وسائل التواصل الاجتماعي المستخدمة في كل انحاء العالم، وحيث الدولة هي المورد الوحيد لخدمات الاتصال، تبقى الانترنت عصية على السيطرة، ويبقى الناس عصاة على التدجين.

فقد أنشأت الصين، عازلا عن الشبكة العالمية للمعلومات، سمي Great Fire wall[186]، شبكات اجتماعية خاصة بها، لتحل مكان الفايسبوك، والتويتر، واليوتيوب، ومنعت اتاحة خدمة المدونات، على غوغل، تحت وطأة التهديد بمنع استخدامه. وإذا كانت الإحصاءات، التي تشير إلى وجود ما يتجاوز الخمسة وثلاثين مليون مستخدم صيني للفايسبوك، غير دقيقة، الا ان لجوء ملايين الصينيين إلى برامج البروكسي، وتجاوز الحظر، يبقى واقعا، ويمكنه ان يخرج الانترنت عن سيطرة الحكومة، في اي وقت.

إذا، وانطلاقا من التجارب التي عرضناها، في مواجهة الإرهاب، يمكن القول، انه قد حان الوقت، لمبادرة الدول العربية الى:

- وضع الاطر اللازمة تنظيميا وتشريعيا، لضمان تعاون فاعل فيما بينها، على المستوى السيبراني، يحمي مواطنيها، واقتصادها، ومجتمعها من الأخطار السيبرانية، والجريمة، والإرهاب بشكل خاص.
- إقرار سياسات دفاع سيبرانية، تأخذ بعين الاعتبار، تجهيز البنى التحتية، وتطوير برامج متخصصة، يمكنها مواجهة الأخطار التقنية العديدة، وضرورة بناء القدرات، وتعزيز مراكز المواجهة الأمنية.
- إنشاء شبكة من اجهزة الوكالات الوطنية للأمن السيبراني، ومراكز طوارئ الانترنت، واجهزة

[186] *The last thing we want to see is people saying that Chinese netizens have free and open access to social media around the world. They don't! They are prevented from looking at many foreign web sites and they are also prevented from accessing information on Chinese web sites! Chinese netizens, for example, are unable to search for "Xi Jinping", the country's next leader, on Sina Weibo, a leading Chinese microblog. The great firewall is not some myth, it's a sad reality. http://thenextweb.com/asia/2012/09/28/no-way-jose/#gref*

إعلامية تعنى بمتابعة ما يحدث في الفضاء السيبراني، وترد على الحملات الدعائية. على ان ترتبط هذه الشبكة، بجهاز عربي موحد للأمن السيبراني، تمثل فيه جميع الدول الأعضاء، ويتولى بدوره تنسيق الجهود، ووضع استراتيجيات الدفاع، والهجوم المضاد، عند الحاجة.

- التعاون مع الهيئات الدولية، والمنظمات المتخصصة في الأمم المتحدة، ومع الدول ذات التجارب الناجحة.
- إنشاء مواقع متخصصة على الشبكات الاجتماعية، يتولاها بشكل أساسي، عناصر من الشباب.
- إنشاء مركز ابحاث عربي متخصص، يكون تابعا للجهاز العربي للأمن السيبراني، الذي سبق واقترحنا انشاوءه، في مسودة مقترح الاتفاقية العربية للأمن السيبراني[187]، يتولى رصد وتوثيق وتحليل المخاطر السيبرانية، والجريمة كما الاعتداءات السيبرانية، ويعد نشرات ودراسات، حول هذا الموضوع.

٦. جهود مشتركة في مواجهة الإرهاب السيبراني

نظرا لطبيعة الانترنت العابرة للحدود، يعتبر التعاون الدولي الفاعل، أحد أهم عناصر نجاح الملاحقات والمحاكمات المرتبطة باستخدام الانترنت لاغراض ارهابية.

وقد أكد الامين العام للامم المتحدة، بان كيمون، ان الانترنت هي المثال الاهم على كيفية عمل الارهابيين بطريقة عابرة للحدود الوطنية، وعليه، تحتاج الدول الى ان تفكر وتعمل بطريقة مماثلة. وقد ورد هذا التأكيد في مقدمة تقرير صادر عن مكتب الامم المتحدة المعني بالمخدرات والجريمة، صادر في العام ٢٠١٢، تحت عنوان "استخدام الانترنت لاغراض ارهابية"[188]. ويتألف هذا التقرير من مئة وثمانية وخمسين صفحة، توزعت على ثماني عناوين، انتهت الى التأكيد على اهمية التعاون الدولي، والاقليمي، والوطني، على كافة المستويات: الرسمية وغير الرسمية، في مواجهة الارهاب.

الا أن غياب الإطار التشريعي الدولي، الذي يحكم موجبات الدول، في مجال التعاون الدولي، لمكافحة الجريمة والارهاب، يؤثر سلبا على فاعلية هذا التعاون، في مواجهة الارهاب، لاسيما على مستويات التحقيق والتنفيذ.

ويشكل هذا الإطار، حاجة ملحة لنجاح جهود التعاون في المكافحة، ما تؤكد عليه، مختلف بروتوكولات التعاون، والاتفاقيات الدولية والاقليمية، سواء منها تلك الخاصة بمكافحة الجرائم العابرة للحدود، أو تلك الخاصة بمكافحة الارهاب، والتي تلحظ آليات تنسيق وتعاون تلزم الدول بوضع سياسات واطر تشريعية وتنظيمية تسهل التعاون، انطلاقا من مستويات الملاحقة، مرورا بالتحقيق، وصولا الى المحاكمة وتنفيذ العقوبات.

الا ان الاطر الدولية للتعاون، ليست كافية، ويفترض بالدول ان تعمد الى ادراج هذه الاطر ومبادئ

[187] مرفقة مع الدراسة
[188] *UNITED NATIONS OFFICE ON DRUGS AND CRIME Vienna - The use of the Internet for terrorist purposes-*
"The *Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner."*
http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

التعاون في تشريعاتها الوطنية. كما يفترض بها أيضا، انشاء الاجهزة الخاصة، التي يتطلبها التنفيذ، وبناء قدرات الموارد البشرية، في الضابطة العدلية والقضاء. على خط متصل، تعتبر الاطر التشريعية للتعاون، في مكافحة الانشطة الجرمية العابرة للحدود، غير كافية هي الاخرى، في غياب هيئة مركزية تتولى التنسيق، وتتخذ المبادرات، لإيجاد الآليات القانونية والعملية لترجمة ارادة التعاون، بشكل عملي.

خارج إطار التعاون الرسمي، والادوات التشريعية المنظمة له، تعتبر الثقة بين الاطراف المتعاونة، من اهم عناصر نجاح هذا التعاون. ويضاف اليه، المبادرات المحلية، والاقليمية، والدولية الهادفة الى تعزيز قدرات القوى الامنية والسلطات القضائية المختصة.

كذلك، لا بد للدول، من اللجوء الى الاستثمار في امكانات التعاون غير الرسمي، وفي شبكات التعاون الامنية التي تنتشر حول العالم[189]، مثل مراكز الاستجابة لطوارئ الانترنت[190]، والى ارساء قواعد خاصة، رسمية وغير رسمية، تتيح التحقيقات المشتركة. فلا شيء يمنع مثلا، من التعاون المباشر مع مزودي الخدمات في بلدان اجنبية، للطلب منهم ان يحتفظوا ببيانات الاتصالات لمدة معينة، وان بطريقة غير رسمية. بينما يقتضي الانتباه، الى ضرورة اللجوء الى السلطات القضائية المختصة، في حالات الاعتماد على البيانات الخاصة بالانترنت، كادلة ثبوتية في المحاكمات الجنائية، وذلك في كل ما يتعلق بآليات معالجتها، من حفظ، وبحث، ومصادرة. وهنا، لا بد للسلطات القضائية، ان تلحظ آليات تنظيمية تضمن القوة الثبوتية لهذه البيانات، لاسيما لناحية حفظها بطريقة تضمن أخذ المحاكم بها، عند الحاجة. ومن هنا ضرورة إيجاد آليات علاقات رسمية وغير رسمية، بين الاجهزة الامنية والقضائية، ومزودي الخدمات، سواء منهم اولئك الخاضعين للسيادة الوطنية، أو اولئك الخاضعين لسيادة اجنبية، بما يضمن ضبط البيانات والحصول عليها، بأسرع وقت ممكن، في التحقيقات الجنائية. ومعلوم ان العديد من القوانين الوطنية، تفرض على مزودي الخدمات، موجب الاحتفاظ ببعض انواع بيانات الاتصال عبر الانترنت، لمدة محدودة. الا انه، خارج الإطار الأوروبي، لا يوجد اتفاق دولي، على نوعية هذه البيانات، أو مدة الاحتفاظ بها.

فبيانات استخدام الانترنت، شديدة الاهمية في التحقيقات الجنائية الخاصة بالارهاب، كما انها أساسية في دعم الاثبات.

من هنا، تبقى فعالية التعاون لناحية تبادل المعلومات، مرتبطة من جهة اولى، بنوعية البيانات ومدة الاحتفاظ بها، ومن جهة ثانية، بحاجة الدول المختلفة، الى حماية البيانات الحساسة، سواء منها تلك الخاصة بالافراد أو بالادارات الرسمية. كما يبقى جمع الادلة الرقمية، مشروطا بحرص الدول على سيادتها، ما يستدعي التنسيق المبكر، والمستمر، بين السلطات المعنية في كل من البلاد المعنية، لمواجهة مشكلة وصعوبة الحصول على بيانات الاتصال بالانترنت عندما تكون موجودة، خارج الحدود الوطنية.

يضاف الى هذا، الصعوبات الناشئة، عن رفض السلطات الوطنية الخاصة بحماية البيانات الشخصية والحريات، اعطاء اذن افشاء البيانات، أو تبادلها مع سلطات بلد آخر.

---

[189] *Network Situational Awareness (NetSA)*
http://www.cert.org/netsa/index.cfm
[190] *http://www.cert.org/incident-management/national-csirts/national-csirts.cfm?*

ففي قضايا الارهاب، حيث تنفذ بعض الافعال المكونة للجرم على الانترنت، تبرز العديد من الإشكالات القانونية والقضائية، لاسيما عندما يستخدم المشتبه به، المقيم في بلد معين، خدمات ومواقع الانترنت، التي يديرها مزود خدمات، مقيم في بلد آخر، لتنفيذ اعماله الجرمية أو الارهابية. كان ينشئ او يدير مواقع تحث على الجهاد، واعمال عنف اخرى، متصلة بالارهاب.

ففي القانون الدولي، لا وجود لقواعد تحدد آليات واصول عمل البلدان، في قضايا جنائية، تتعدد فيها الصلاحية القضائية، بحيث يكون أكثر من قانون وطني، واجب التطبيق، على مشتبه به واحد، ومن هنا ضرورة التنسيق المبكر بين الدول لحل صعوبات ومشكلات الصلاحيات.

الفصل السابع
التعاون لتحقيق الأمن السيبراني

١ . إلزامية التعاون

أ- عالم مترابط ومعرض للمخاطر

فيما تشكل الشبكات السلكية واللاسلكية، المحور الذي نبني حوله، ونؤسس نشاطاتنا ومجريات حياتنا اليومية، يطرح السؤال حول ما إذا كنا مستعدين للتعاون معا في حماية هذه الشبكات. وإذا كانت بعض البلدان قد نشطت في مجال مكافحة الجريمة السيبرانية والجريمة المعلوماتية، بما فيها الغش السيبراني، والاختراقات والتجسس، والرقابة، والإرهاب، فان بعضها، لاسيما في محيطنا العربي، لم يحرك ساكنا إلى الآن، كلبنان مثلا، حيث لا اطر قانونية، ولا مواكبة ادارية، ولا اجهزة متخصصة في تبادل المعلومات، حول الاختراقات والجرائم، وأفضل الممارسات.

كل ذلك، بالرغم من اننا نعيش اليوم، في العصر السيبراني، حيث العالم مترابط، متصل بشكل دائم، ومعرض للمخاطر، بشكل غير مسبوق، نتيجة اعتمادنا المتنامي على تقنيات المعلومات والاتصالات، وقد دخلت في أدق تفاصيل حياتنا اليومية، العملية والشخصية. وبات من الصعب على أي شخص في هذا العالم، ان يعزل نفسه عن هذا المجال، بحجة عدم استخدامه للانترنت، ذلك ان البنية التحتية لكل الخدمات التي تقدم له، انطلاقا من الطاقة والموارد المائية، مرورا بالخدمات الادارية، وصولا إلى استخدامه لوسائل النقل، والخدمات الحيوية، تعتمد على تقنيات المعلومات والاتصالات.

فالجريمة، مثلا، وجدت فيه آفاقا أكثر اتساعا، والمجرمون توسلوه، للحد من مخاطر الانكشاف، والوقوع في يد العدالة. لذا، لا يمكن لاي دولة، ان تنأى بنفسها عن هموم الأمن في هذا المجال، حيث الاختراقات والاعتداءات، قد تطاول، ايا كان، عبر المروحة الواسعة لاجهزة الاتصال، بالشبكة العالمية للمعلومات.

والجريمة التي تستخدم تقنيات المعلومات والاتصالات، أو التي تستهدفها، تعرض الأفراد، والمؤسسات، والدول، لخطر داهم.

فقد تنبه المجرمون إلى اهمية البيانات، ومعطوبية الأنظمة، وامكانات جمع الأموال، بطرق أكثر سهولة، كما تنبهوا إلى طبيعة هذا المجال المفتوحة، والى صعوبة تطبيق الاطر التنظيمية والتشريعية التقليدية، أحيانا كثيرة، لاعتبارات متعددة، ليس أقلها عدم وجود إطار تشريعي متكامل للفضاء السيبراني، وغياب التعاون الفاعل بين الدول، والذي يسمح بملاحقتهم عبر الحدود، بالرغم من بروز عدد لا بأس به من الجهود الدولية، والإقليمية لمكافحة الجريمة السيبرانية.

ب- جريمة عابرة للحدود

الجريمة السيبرانية، كأي عمل سيبراني آخر، ذات أبعاد عالمية، كونها تتجاوز بمفعولها ومداها، أشخاصا أو أموالا، في الامكنة المختلفة التي يمكن ان تصل اليها، والتي تقع تحت اختصاصات قانونية مختلفة، ما ينعكس على التوصيف القانوني، وإجراءات التحقيق واصولها، والصلاحية، والأدلة الموجودة والمحفوظة، على اراضي اجنبية، الامر الذي يفرض تعاونا بين السلطات المختصة، في عدد من البلدان، للوصول إلى نتيجة، سواء على مستوى المتابعة والملاحقة وجمع الأدلة، أو على مستوى إنزال العقاب.

وتأخذ الجريمة طابعا عابرا للحدود، في كل مرة ينطلق فيها النشاط الجرمي، من بلد معين، ليصل إلى بلد آخر، أو ليعبره إلى بلد ثالث. وفي كل مرة، يظهر فيها أحد عناصر الجريمة، أو نتائجها، في مكان جغرافي آخر، خاضع لنظام قانوني، وصلاحية قضائية مختلفة، أو عدد من البلدان. فاصول التحقيق، تفرض تتبع النشاط الجرمي، ما يترجم، بملاحقة خط سير العمل منذ نقطة الانطلاق، وحتى نقطة أو نقاط الوصول. وعليه، تلعب السجلات التي تحفظ آثار العمل، وخط مسيره، دورا هاما، في الوقت الذي يمكن ان تتواجد فيه، على اراض دول مختلفة. ولا يخفى ضرورة اللجوء، خلال التحقيق، إلى قنوات الاتصال، ومقدمي خدمات الانترنت؛ وجميعها يمكن ان يكون خاضعا لسيادة مختلفة، وإجراءات قانونية متباعدة.

وغالبا ما يؤدي التحقيق، كما الملاحقة في الجرائم السيبرانية، إلى الدخول إلى أنظمة معلومات، والاطلاع على بيانات ومعلومات، مخزنة على خوادم في منطقة جغرافية، غير خاضعة لسيادة الدولة التي تقوم بالتحقيق، ومن دون الحصول على موافقة الدولة المعنية. وهذا ما سيحدث بتواتر أكبر، مع انتشار الحوسبة السحابية، وتوسع استخدامها، لاسيما مع اعتمادها على تقنية حفظ المعلومات في مراكز بيانات، في عدد من البلدان، خاضعة لأنظمة قانونية مختلفة، وسيادة مختلفة.

وكانت القوانين التقليدية، قد تعاملت مع هذا الموضوع، بإقرار الصلاحيات المكانية والذاتية والشخصية والشاملة. وقد اتجهت معظم الدول، في مجال الجريمة السيبرانية، إلى اعتبار مكان وقوع الجرم، كما جنسية المجرم، صلة ارتباط كافية، بين الأعمال الجرمية السيبرانية وإحدى الدول على الأقل، بحيث تتحدد الصلاحية على أساسها.

وبالفعل، فقد تنبهت الدول المختلفة، منذ البداية، إلى ان مكافحة الجريمة السيبرانية، تفرض مقاربة تتناسب وطبيعتها التقنية، والعابرة للحدود. فالأطر القانونية الوطنية، على الرغم من اهميتها، تبقى غير فاعلة، في غياب التعاون الدولي، الذي يضمن انسجاما على مستوى تعريف الجريمة السيبرانية، وتحديدا لآليات تعاون عبر الحدود، بما يؤسس لتعاون دولي، وفي غياب مقاربة إقليمية للمسائل الخاصة، التي يمكن التوافق عليها، في منطقة معينة، دون أن يكون ذلك ممكنا بالضرورة، على المستوى الدولي. ويبدو هذا الوضع الأخير صحيحا، بالنسبة للعديد من قضايا المحتوى، التي غالبا ما ترتبط بخصوصية المجتمع، كما بالمعتقدات والأديان، على سبيل المثال.

ج- خطورة غياب التعاون

يجمع المتخصصون والخبراء، على خطورة التباعد والانقسام، في مكافحة الجريمة السيبرانية، على المستوى الدولي، وعلى اعتبار تنوع واختلاف التشريعات الوطنية، عائقا أمام التعاون الدولي[191]. وكانت مجموعة العمل في مكتب مكافحة المخدرات والجريمة، لدى الأمم المتحدة، قد رفعت تقريرا بهذا المعنى، حول الجريمة السيبرانية وتعامل الدول الأعضاء معها. في المقابل، اعتبرت القواعد القانونية، في الاتفاقات متعددة الاطراف، فاعلة في مكافحة الجريمة[192]، لاسيما وإنها تعزز قدرة التشريعات الوضعية، وأصول الملاحقة والإجراءات الوطنية، إضافة إلى إتاحتها امكانية الانسجام مع التشريعات الدولية، حول الموضوع، الأمر الذي يمكن أن يؤسس، لتعاون فاعل.

ففي مواجهة تعاون المجموعات الإجرامية، وإفادة الجريمة المنظمة، من تقنيات المعلومات والاتصالات، في تسهيل أعمالها، وتبادل البيانات والخدمات، وربط مجموعاتها المنتشرة في بلدان مختلفة[193]، لا بد من شبكة تعاون، بين مختلف الدول، والسلطات القضائية والأمنية، تعيد التوازن إلى قدرة الجهات الرسمية والحكومية، على المواجهة.

الا أنه، لا يمكن لاي إطار تعاون، ان ينجح، في غياب تطابق الأولويات الرئيسية لدى البلدان الشريكة، لانه يؤثر سلبا على التزامها، وعلى استدامة التعاون نفسه، وفعاليته وكفاءته. ولعل الدليل الاقرب، تاخر السوق العربية المشتركة، لاستبعادها كأولوية على أجندات الحكومات العربية المعنية، مقابل نجاح التكتلات الخليجية حول استثمار النفط وإدارة موارده، حيث حل كأولوية في قائمة اهتمامها.

وإذا كان العديد من دول المنطقة، لم تبرم اتفاقية عربية للأمن السيبراني، و لم تعتمد القانون النموذجي الذي اعدته جامعة الدول لعربية، لمكافحة الجريمة السيبرانية، فان الوقت قد حان للمبادرة فورا، إلى إيجاد سبل لإقرار التشريعات الوطنية الملائمة، والمتجانسة، واعتماد آليات تعاون تقني وفني وقضائي، تضمن استقرار المجتمعات والدول، وتؤسس لتفاهم على المسائل الإقليمية المشتركة، لاسيما على مستوى الجرائم الخاصة بالمحتوى، ولدور فاعل للمنطقة العربية، على المستوى الدولي. كذلك، لا بد من إيجاد مراكز اتصال دائم، بين الأجهزة الأمنية المعنية بالملاحقة، وبالأمن، بحيث ترصد الاعتداءات والاختراقات قبل وقوعها، ويمكن الحد من آثارها، بأكبر قدر ممكن.

د- أهمية التعاون

تتراكم العناصر التي تجعل المجال السيبراني، مجالا خطرا، وصعب المراس، ما يجعل السيطرة على ما يحدث فيه، صعبة المنال، وغير فاعلة، ونذكر على سبيل المثال: الامتداد العالمي للشبكة، عدم وجود توافق دولي، على القواعد الواجبة التطبيق، على سلوك الدول في هذا المجال، سهولة ارتكاب الاعتداءات ونتائجها الكارثية، كانتشار الفيروسات، واصابة الأنظمة غير المعنية وغير المستهدفة بالهجوم. يضاف

[191] *Comprehensive Study on Cybercrime Draft—February- 2013. http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf*

[192] *Membership of a multilateral cybercrime instrument corresponds with the perception of increased sufficiency of national criminal and procedural law, indicating that current multilateral provisions in these areas are generally considered effective.*

[193] *White house strategy to combat transnational organized crime. "Virtually every transnational criminal organization and its enterprises are connected and enabled by information systems technologies, making cybercrime a substantially more important concern."http://www.whitehouse.gov/administration/eop/nsc/transnational-crime/introduction*

إلى ذلك، المجهولية التي تساعد على اخفاء الجهة المعتدية، أو تساعد في تعقيد عملية الوصول اليها، أو حتى، يمكنها ان تؤدي إلى نسب الاعتداء إلى جهة غير الجهة المعتدية. هذا، دون ان ننسى الثغرات المعلوماتية، في العديد من البرمجيات المستخدمة. وتشكل تقنيات المعلومات والاتصالات مصدرا مقلقا للمخاطر، لا يمكن مواجهته، خارج إطار التعاون الدولي. وكان الامين العام للامم المتحدة قد اكد على اهمية هذا التعاون في مناسبات عدة[194].

وهكذا، تتزايد امكانات ووسائل الاعتداء على البنية التحتية للمعلومات والاتصالات، والسيطرة عليها، وتتوسع المخاوف، حول القوانين الواجبة التطبيق في الفضاء السيبراني، ما يؤسس لنزاعات دولية، وحروب، ويدرك صناع القرار في العديد من البلدان، مدى قوة تقنيات المعلومات والاتصالات، على كسر الحواجز وتطوير الاقتصاد، تماما، كما يدركون آثارها السلبية والخطيرة، والتي ليس لأية دولة القدرة على تحصين نفسها، في مواجهتها، منفردة.

ففي عصر الشبكات، لم تعد الجغرافيا درعا للوقاية من التحديات العالمية، حيث يتشاطر العالم اليوم هموما أمنية مشتركة، هي الأخطار السيبرانية. ولذلك، أضحى التعاون هو النموذج الأمني الجديد في عصرنا هذا، حيث أصبح الأمن متشابكا بوتيرة متزايدة، وأصبح الدفاع يتطلب مزيدا من العمل، مع الدول والمؤسسات والمنظمات.

من هنا، يبدو ضروريا أن تلعب الأمم المتحدة، دورا ايجابيا في تحقيق السلام السيبراني، لاسيما وأنها، المعنية الأولى بالسلام، في العالم، وبالحد من النزاعات بين الدول. في هذا الإطار. في العام ٢٠١٢، عين بان كيمون، الامين العام للامم المتحدة، فريقا من الخبراء، تألف من ١٥ دولة، من بينها الأعضاء الدائمون في مجلس الأمن، لدراسة إجراءات التعاون الممكنة لمواجهة المخاطر السيبرانية. وفي التقرير الذي رفعه الخبراء في العام ٢٠١٣، والذي جاء تحت ثلاث عناوين أساسية، برزت مبادئ حول:

- تطبيق القانون الدولي على سلوك الدول في الفضاء السيبراني.
- توسيع مدى تطبيق القواعد التقليدية حول الشفافية وبناء الثقة.
- توصية بالتعاون الدولي وبناء القدرات لجعل البنية التحتية للمعلومات والاتصالات حول العالم، أكثر أمنا.

وقد أبرز التقرير، المخاطر الناتجة عن انتشار الاعتماد على تقنيات المعلومات والاتصالات، في البنية التحتية، لاسيما في مجال أنظمة إدارة ومراقبة المفاعلات النووية. وتبقى اهمية التقرير، فيما يمثله من سابقة، في مجال التوافق بين الدول على مجموعة من التوصيات حول المعايير، والقواعد، ومبادئ مسؤولية الدول في المجال السيبراني، ما يؤسس لنواة قانون دولي في هذا المجال. ويسمح بالتوجه نحو الإقرار بتطبيق القوانين الدولية، في غياب الإطار القانوني الخاص، وبتطبيق شرعة الأمم المتحدة، على الدول الأعضاء، وباتاحة المجال امام الدول التي تتعرض لاعتداءات لمراجعة الأمم المتحدة، وأجهزتها المختصة.

[194] *A/70/174- "Few technologies have been as powerful as information and communications technologies (ICTs) in reshaping economies, societies and international relations. Cyberspace touches every aspect of our lives. The benefits are enormous, but these do not come without risk. Making cyberspace stable and secure can only be achieved through international cooperation, and the foundation of this cooperation must be international law and the principles of the UN Charter*
https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf

كذلك، يمكن البناء على ما تقدم، للخروج باتفاقيات دولية وإقليمية وثنائية، تنظم العلاقات بين الدول، والتعاون فيما بينها، لمواجهة المخاطر السيبرانية، ومنع تحولها إلى سبب لاشتعال الحروب السيبرانية، التي يمكن أن تترجم بكوارث تطال العالم أجمع.

فالدول الأعضاء، ملزمة بحسب هذه الشرعة، باحترام سيادة الدول الاخرى، واستقلالها، كما هي ملزمة بالامتناع عن استخدام القوة، وباللجوء إلى الوسائل السلمية في حل النزاعات. وإذا كان التقرير، لم يورد تحديدا لما يمكن اعتباره، هجوما سيبرانيا بمستوى الإعداء المسلح، الذي يجيز للدولة المعتدى عليها استعمال حق الرد، أو ما يمكن اعتباره ردا مناسبا، الا أنه أسس لتطبيق القواعد التقليدية بشكل مناسب، لاسيما فيما يتعلق بمنع الدول من الاعتداء على حقوق الملكية الصناعية والفكرية للأفراد في الدول الاخرى، واستثمار بياناتهم الشخصية، والاعتداء على ى حياتهم الخاصة، لاسيما وان هذا الامر، يعتبر اعتداء على سلامة الدولة وامنها القومي.

الا أن كل ما تقدم، يفترض من وجهة نظر قانونية، اثبات تورط الدولة في الاعتداء، ووقوفها خلفه، أو تحريضها على القيام به. اذ يمكن الا تقوم اجهزة في الدولة بهذا الهجوم، وانما منظمة أو مؤسسة تابعة لها، أو مأجورة منها. ويستدعي هذا الاثبات، الالتفات إلى الجوانب التقنية، والوسائل التي يمكن اعتمادها للاثبات، وتتبع الاثر، وتأكيد انطلاق الاعتداء من جهاز تابع للدولة، من خلال أحد الأشخاص التابعين لها، أو من خلال اجهزة خاصة، استخدمت من قبل أشخاص تابعين للدولة وبأمر منها الخ...

وتفهم اهمية هذا التقرير والتعاون، كجهد وخطوة عملية هامة، باتجاه التأسيس لمجال سيبراني سلمي، ولمنع عسكرته، على ضوء ما ورد في دراسة لمعهد الابحاث حول نزع السلاح التابع للامم المتحدة، عن تجاوز عدد الدول التي طورت قدرات قتالية سيبيرانية، الاربعين دولة، وعن كون اثنا عشر منها، قد طورت قدرات هجومية[195]. كما من خلال تفاوض الدول بين بعضها، لإيجاد اطر تنظيمية وتشريعية ودبلوماسية تضمن بناء الثقة في العالم السيبراني، عبر التعاون في تبادل المعلومات حول التهديدات، والازمات. فقد اتفقت كل من الولايات المتحدة وروسيا، مثلا، نتيجة مفاوضات بينهما، على تحديد طرق التعاون في الازمات السيبرانية، عبر خط ساخن، ومراكز الرد على طوارئ الانترنت، والاتصال بين المراكز النووية لمواجهة الاعتداءات السيبرانية[196]. كما تسجل في هذا المجال، مناقشات الفريق الأميركي الصيني[197]، الامر الذي يساعد على تقدم التوافق الدولي، حول قواعد واصول التعامل بين الدول، في العالم السيبراني.

[195] *http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf*
[196] *UNIDIR, "Cyber Index," pp. 125-138*
[197] *http://www.state.gov./r/pa/prs/ps/2013/07/211862.htm*

٢. بين القوانين المحلية والقانون الدولي

يعتبر القانون الوسيلة الأولى، في تنظيم التعاملات بين أفراد المجتمعات المختلفة، وإحدى الوسائل الهامة، في تنظيم العلاقات بين الدول، سواء لتأمين الاستقرار ومنع النزاعات والحد منها، أو لحماية الحقوق ومنع الجريمة. لذا كان من الطبيعي، ان تهتم الحكومات المختلفة، بوضع إطار تشريعي وتنظيمي، لترتيب الاوضاع الجديدة، الناشئة نتيجة لبروز نشاطات جديدة، واشكال جديدة من الجرائم، رافقت التحول نحو مجتمع المعلومات والمعرفة. فلطالما حكمت القوانين الوطنية، والقوانين الدولية، العديد من الاوضاع والحالات، والعلاقات بين الدول، بما يحقق حماية المجتمعات، لاسيما في المجالات التي تطاول مجتمعات متعددة، أو التي يمكن ان تعني الإنسانية ككل، والتي يمكن ان تقع تحت اختصاصات قضائية مختلفة، مثل النقل الدولي، والاتصالات، والجريمة المنظمة، والجريمة العابرة للحدود، والفضاء الخارجي. ولا تخرج الجرائم السيبرانية عن هذه القاعدة، حيث لا بد من تطبيق القوانين الوطنية، والقانون الدولي، والاتفاقات المتعددة والاطراف، والثنائية، كما العلاقات الدبلوماسية.

الا ان الطبيعة التقنية والجديدة، كما خصوصية الجريمة السيبرانية، تلزم الدول إيجاد القواعد القانونية المناسبة، عند قصور القوانين التقليدية، على المستوى الوطني، واطر وآليات التعاون مع الدول الاخرى، لتأمين إطار مناسب لهذه الجريمة العابرة للحدود، كما لما ينتج عنها من أدلة إلكترونية، ذات طبيعة مختلفة عن الأدلة التقليدية، وما يرتبط بها من آليات جمع وتدقيق. كذلك، ولنجاح التعاون، لا بد من العمل، على تحقيق الانسجام، بين القوانين والقواعد الخاصة بمكافحة الجريمة السيبرانية، منعا لبروز الجنات الجرمية، وتسهيل التعاون.

وتقوم فلسفة التعاون بين الدول، في المجال القانوني، بشكل أساسي، على تطويع مبدأ سيادة الدول، والاختصاص القانوني والقضائي، الذي يرتبط به، من خلال اعتراف الدولة، بحق دولة اخرى، بالقيام بالتحقيق، على أراضيها.

ويتخذ التعاون في المجال القانوني، صورا مختلفة، مثل تسليم المجرمين، والمساعدة القضائية، والاعتراف المتبادل بقوة القضية المحكمة، وتنسيقا غير رسمي بين الأجهزة العسكرية والأمنية المعنية. ونظرا لطبيعة الأدلة الإلكترونية، والتي تتطلب ردا فوريا، يفترض الحصول على المعلومات الضرورية لذلك، الامر الذي يعني قدرة على إطلاق عملية تحقيقات متخصصة، كرصد الاتصالات، ومتابعتها، والحفظ الآني للبيانات. وتلجأ الدول، في غالب الاحيان، إلى طلب رسمي من الدول الاخرى، للحصول على البيانات، لاستخدامها كدليل في اثبات الجرم، وذلك ضمن إطار من الاتفاقات الثنائية، التي تنظم التعاون فيما بينها. ولكن اللجوء إلى هذه الآلية التقليدية، يتطلب وقتا طويلا، نسبيا، يمكن ان يمتد لشهور، وهذا ما لا يتناسب وطبيعة الجريمة السيبرانية، كما وطبيعة الأدلة التي يفترض ان تجمع لاثباتها، الامر الذي يوجب إيجاد آليات وقنوات للتعاون، تضمن سرعة التجاوب والرد الفوري، ليس على المستويين الإقليمي والدولي.

٣. الجهود الإقليمية

أ- نظرة عامة

يعتبر التعاون بين الدول، بشكل عام، والتعاون الإقليمي، بشكل خاص، عن طريق إقرار الاتفاقيات الإقليمية، أداة لتحفيز الحوار السياسي وحفظ الاستقرار، وتنفيذ المشاريع الإقليمية، وتلبية لاحتياجات البلدان الشريكة، وتطوير القدرات، وتثمير الامكانيات، ومعالجة المشاكل والأولويات الخاصة بدول تتشارك إقليما جغرافيا، أو قواسم ثقافية واجتماعية ولغوية. ويمكن للتعاون ان يشمل الهموم الاقتصادية، بهدف تعزيز الوضع المعيشي، والقدرة الاقتصادية للشعوب، كما يحصل منذ العقد الماضي، في مجالات عديدة، مثل النقل، والموارد المائية والكهربائية، والأمن.

ولعل أهم ما يؤشر إلى وعي الحكومات المختلفة، لاهمية التعاون الإقليمي، على المستوى العربي، هو إنشاء عدد من المنظمات كجامعة الدول العربية، والمنظمة الاسلامية للتربية والعلوم والثقافة، ومجلس التعاون الخليجي، والبنك الاسلامي للتنمية.

يضاف إلى ذلك، ما يبذل من جهود، في بقاع العالم كله، للتعاون على المستويات الأوروبية، والأميركية، والفرانكوفونية، والكومنولث. كما ترد هنا، الأموال التي تخصص لبرامج التعاون الإقليمي، وليس أقلها ما خصصته المفوضية الأوروبية خلال الفترة ٢٠٠٤ ــــ ٢٠١٠، بحيث بلغ مجموعه ٩,٦ مليار يورو، افادت منها البلدان المنخرطة، في سياسة الجوار الأوروبية.

ففي كل مرة يظهر فيها هم دولي، أو إقليمي مشترك، تظهر الدول ميلا إلى التعاون. ولا يخرج هم مكافحة الجريمة السيبرانية عن هذه القاعدة. لذا نجد ان العالم، ممثلا بالأمم المتحدة، يدفع بهذا الاتجاه، كما نلاحظ بروز العديد من المبادرات والجهود، التي تصب في خانة ارساء قواعد التعاون. ولكن هل تكفي الاتفاقيات الإقليمية في هذا المجال؟ هذا ما سنحاول الاجابة عليه، من خلال استعراض بعض الاتفاقيات، لاسيما منها اتفاقية بودابست، كونها الاداة الأولى، التي برزت تحت عنوان: التعاون لمكافحة الجريمة السيبرانية.

وتنسجم الاتفاقات الإقليمية مع متطلبات مواكبة طبيعة وسرعة النشاط الجرمي، في المجال السيبراني، كما مع طبيعة الأدلة والآثار المترتبة عليه. ويسجل في هذا المجال، عدد من المبادرات[198]، كمبادرة شانغهاي، ومبادرة رابطة البلدان المستقلة، وغيرها، مما سيرد ذكره، لاحقا.

ففي العام ٢٠٠٢، وضعت مجموعة بلدان الكومنولث[199]، التي تضم ٥٣ دولة، قانونا نموذجيا لمكافحة الجريمة السيبرانية، حرصت على ان يأتي منسجما، مع الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية.

[198] *International/Regional Initiatives. Commonwealth of Independent States: Agreement on Cooperation in Combating Offences related to Computer Information (2001). Commonwealth: Model Laws on Computer and Computer-related Crime (2002)/ Electronic Evidence (2002)/Harare Scheme (2002/2011) - Shanghai Cooperation Organization: Agreement on Cooperation in the Field of Information Security (2009) - League of Arab States: Convention on Combating Information Technology Offences (2010) Caribbean*: *ITU/Caribbean Community/CTU Model Legislative Texts on Cybercrime, e-Crime and Electronic Evidence (2010) Pacific*: *ITU/Secretariat of the Pacific Community Model Law on Cybercrime (2011)*
(Draft) *EAC Legal Framework for Cyberlaws (2008) (Draft) ECOWAS Directive on Fighting Cybercrime (2011) COMESA Cybersecurity Draft Model Bill (2011) (Draft) African Union Convention on the Establishment of a Legal Framework Conductive to Cybersecurity in Africa (2012) SADC Model Law on Computer Crime and Cybercrime (2012)*
[199] *Commonwealth of Nations*

كما وضعت قانونا نموذجيا آخر، حول الاثبات الرقمي، نظرا لأهمية الاثبات في القانون. فالى جانب القوانين الوضعية، لا بد من إجراءات وأصول، تضمن الوصول إلى الإدانة، أو إلى إثبات البراءة[200]. كما لا يمكن لأي محكمة، ان تعمل دون أدلة اثبات.

وفي العام ٢٠٠٩، بادرت المجموعة الاقتصادية لغرب افريقيا[201]، المؤلفة من ١٥ دولة عضوا، إلى إقرار توصية لمكافحة الجريمة السيبرانية، تشكل الإطار القانوني لعمل الدول الأعضاء. وقد تضمنت هذه الاتفاقية، إضافة إلى المواد التجريمية، موادا خاصة بالاصول والإجراءات، بحيث غطت مسألة الاثبات، والأدلة الرقمية.

تبع ذلك، مبادرة من قبل السوق المشتركة لشرق وجنوب افريقيا، في العام ٢٠١١، لوضع قانون نموذجي[202]، حول مختلف جوانب الجريمة السيبرانية.

وكان الاتحاد الدولي للاتصالات، والاتحاد الأوروبي، قد اشتركا في دعم وضع قانون وسياسة نموذجيين، في العام ٢٠١٠[203]، قام باعدادهما عدد من الخبراء، من منطقة الكاريبي، بحيث اعتمدا لوضع القوانين والسياسات الوطنية، في دول الكاريبي، كما دعما جهدا مماثلا، لدول المحيط الباسفيكي[204].

على خط مواز، وضعت منظمة الدول الأميركية[205]، عددا من التوصيات حول الجريمة السيبرانية، لكن التنفيذ على المستوى الوطني، لم يتم انجازه بعد.

على المستوى الأوروبي، أقر عدد من التوصيات، واتخذ العديد من القرارات لتحقيق الانسجام، بين التشريعات الوطنية للدول الأعضاء في الاتحاد، والتي تكافح الجريمة السيبرانية. فاقر المجلس الأوروبي، المؤلف من ٤٧ دولة عضو، اتفاقية لمكافحة الجريمة السيبرانية، في العام ٢٠٠١، والبروتوكول الاضافي لها، في العام ٢٠٠٣، كما أقر اتفاقية لحماية الأطفال ضد الاستغلال الجنسي، في العام ٢٠٠٧.

ب- اتفاقية بودابست

شكلت الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية، خطوة رائدة على مستوى التعاون بين الدول، لمواجهة هذا الخطر. وهي الوحيدة حتى اليوم، من حيث حجم الدول المنضمة اليها، ومن حيث مداها. وقد جاءت هذه الاتفاقية، لتكلل جهود مجموعة من الخبراء، الأوروبيين وغير الأوروبيين، كالولايات المتحدة، وافريقيا الجنوبية، واليابان، والتي عملت ضمن مجموعة «خبراء لمكافحة الجريمة في الفضاء السيبراني».

دخلت هذه الاتفاقية حيز التنفيذ، في تموز ٢٠٠٤، بعد ان عرضت للتوقيع ابتداء من نوفمبر ٢٠٠١، كاول اداة إقليمية ملزمة لمكافحة الجريمة السيبرانية، عبر تحقيق الانسجام بين القوانين الوطنية. وقد شددت، بشكل خاص، على تحسين تقنيات التحقيق والبحث، وزيادة التعاون بين الدول.

وقد بلغ عدد الدول التي أقرت هذه الاتفاقية، حتى اليوم، إحدى وأربعين دولة، بينما وقعت عليها إحدى عشرة دولة دون ان تقرها. وكانت هذه الاتفاقية، قد اتبعت ببروتوكول، دخل حيز التطبيق في

[200] *Commonwealth model law on digital evidence- 2002*
[201] *The Economic Community of West African States - ECOWAS - Founded in 1975*
[202] *Cybersecurity Draft Model Bill Model Law - Common Market for Eastern and Southern Africa - Comesa- 2011*
[203] *HIPCAR- Model legislation and policy developed in 2010 by Caribbean experts*
[204] *ICB4PAC- Pacific countries to develop their own model policy and legislation*
[205] *Recommendations of Organization of American States -OAS*

مارس ٢٠٠٦، ويهدف إلى تجريم المحتوى العنصري وكراهية الاجانب على الانترنت، كما لتجريم التهديدات والشتائم المبنية عليهما.

توزعت بنود الاتفاقية، على محاور ثلاثة:

- الانسجام بين التشريعات الوطنية، التي تجرم الأعمال غير القانونية في الفضاء السيبراني
- تحديد وسائل التحقيق والملاحقة الجزائية، التي تنسجم مع الطبيعة العالمية للشبكة
- وضع نظام تعاون بين الدول، يتصف بالسرعة والفاعلية.

وزعت الاتفاقية الجرائم التي ترتكب بواسطة الانترنت، على أربع مجموعات كبرى، تضم الأولى: الجرائم التي تتعرض لخصوصية وسلامة وتوفر الأنظمة والبيانات؛ مثل النفاذ غير الشرعي، والاعتراض غير الشرعي، وتشويه البيانات، وسلامة النظام. وتضم المجموعة الثانية: جرائم التزوير والاحتيال، بينما تندرج في الثالثة، الجرائم المتصلة بالمحتوى، مثل: انتاج، وتوزيع، وحيازة مواد اباحية يستخدم فيها الأطفال، وفي المجموعة الرابعة، جرائم الاعتداء على الملكية الفكرية، والحقوق المجاورة.

ويؤشر إلى نجاح هذه الاتفاقية، والبروتوكول التابع لها، انضمام العديد من الدول غير الأوروبية اليها، واتخاذها صفة الاداة الدولية، بانضمام الولايات المتحدة الأميركية، واليابان، واستراليا، وجنوب افريقيا، وكندا وغيرها. فمع نفاذ هذه الاتفاقية، في كافة الدول التي وقعتها، تتحول إلى اداة لإدارة المخاطر، والتهديدات السيبرانية.

وترتكز اهمية هذه الاتفاقية بفعاليتها على إقرارها إجراءات عملية، تلتزم الدول المنضمة بادراجها في قوانينها الوطنية، مثل تلك الخاصة بجمع بيانات الاتصال وحفظها؛ بما يتيح تحديد مصدرها، ونقطة وصولها، وصلاحية الجهات القضائية المعنية، والمساعدة المتبادلة وتسليم المجرمين.

فقد لحظت المعاهدة، في المادة الثالثة والعشرين، تعاون الاطراف إلى اقصى حد ممكن، لاسيما على مستوى: تبادل المعلومات والأدلة، رصد الاتصالات وتعقبها، وحفظ البيانات ونقلها، وتبادلها، والاطلاع على المحتوى، وبيانات الاتصالات، تفتيش وضبط محتوى الأجهزة المخزن، الجمع الفوري لبيانات الاتصال، التعاون القضائي، تبادل المجرمين، وإنشاء مراكز وحدات خاصة، تؤمن المتابعة وتبادل المعلومات دون انقطاع، على مدار اليوم، كل ايام الاسبوع ٢٤/٧. وتعتبر مراكز الاتصال هذه، حجر الأساس، الذي ترتكز اليه فعالية التحقيق، وتبادل المعلومات.

وتتميز الاتفاقية الأوروبية، بالمتابعة التي تحظى بها، من قبل المجلس الأوروبي، الذي يعقد اجتماعات وندوات بشكل مستمر، سواء لتعديلها، بما يتلاءم أكثر مع واقع الجريمة السيبرانية، كما حصل مع إقرار البروتوكولات اللاحقة لها، أو من خلال تشديده على اهمية التعاون بين الأجهزة المختصة، حيث ركزت على: التعاون بين السلطات القضائية ومزودي الخدمات، ومتابعة آثار عمليات تبييض الأموال على الانترنت، والتعرف على الاشكال الجديدة للمخاطر السيبرانية، وواقع وفعالية التشريعات السيبرانية في مجال مكافحة الجريمة، كما ناقشت فعالية التعاون بين نقاط الاتصال ٢٤/٧.

يضاف إلى ذلك، ما يصدر من توصيات وتوجيهات عملية، لكيفية تطبيق الاتفاقية، بشكل عام، أو في

مسائل معينة. ويذكر هنا أيضا، تعاون المجلس مع اللاعبين الأساسيين في مجال البرمجيات، كما الاتفاق الذي وقع مع مايكروسوفت.

وقد أوردت هذه المعاهدة، بنودا خاصة لحماية الحريات والحقوق، وسمحت بوصول المحققين إلى المعلومات المتاحة للعموم، أو بموافقة وارادة الطرف المعني، بالحفاظ على البيانات.

٤ . التعاون الدولي

مع الانتباه إلى الأبعاد العالمية للاعتداءات وللجريمة السيبرانية، برز الاهتمام بالتعاون الدولي. وانطلقت الفكرة لحماية الفضاء السيبراني، ومواجهة المخاطر، من التجمع الدولي للعلماء[206]، الذي أشار إلى هذا التعاون، كنظام دولي للفضاء السيبراني ، يرعى جميع المسائل الجرمية بما فيها الحرب الإلكترونية. وقد قادت الأمم المتحدة، هذه الجهود، سواء عبر إقرارها تنظيم القمة العالمية لمجتمع المعلومات، أو انشائها مجموعات عمل، لمكافحة الجريمة السيبرانية، واتخاذها العديد من القرارات، التي تدعم الأمن والسلامة، في الفضاء السيبراني.

لعبت القرارات الصادرة عن الهيئة العامة للامم المتحدة، حول الأمن السيبراني وتقنيات المعلومات، دورا في جذب انتباه الدول الأعضاء، إلى أهمية التحديات السيبرانية.

وتسجل حركة ناشطة لعدد من الأجهزة، والادارات، وفرق العمل، التابعة للامم المتحدة، في هذا المجال، على مستويات عدة، حيث يدعم مكتب مكافحة الجريمة والمخدرات جهود الأمم المتحدة، في هذا المجال، حتى على الانترنت، كما تهتم منظمة الجمارك العالمية، بالترويج لاستراتيجيات حماية البنية التحتية الحرجة، بينما تهتم اللجنة الاقتصادية والاجتماعية على تحسين تبادل المعلومات، والممارسات الفضلى، والتدريب على مكافحة الاستخدام الجرمي للشبكة.

كذلك، اصدرت الهيئة العامة للامم المتحدة، قرارا حول ضرورة نشر ثقافة الأمن السيبراني[207]، وضرورة زيادة الوعي والمسؤولية، لدى الدول، بما يضمن التعاون في الوقت المناسب، لمنع، ورصد، ومعالجة الحوادث السيبرانية. بعد ذلك، دعت جميع الهيئات الدولية، والدول الأعضاء، التي وضعت استراتيجيات للأمن السيبراني وحماية البنية التحتية الحرجة، إلى المشاركة على مستوى الممارسات الفضلى، والتدابير، التي تسهل افادة بقية الدول الأعضاء منها[208].

وقد بدا اهتمام الدول بالتعاون واضحا، من خلال مشاركتها في اعمال الجمعية العامة للامم المتحدة، التي ضمت ١٩٢ دولة، والتي اصدرت عددا من القرارات، التي يمكن اعتبارها قاعدة لانطلاق الجهود، في مكافحة الجريمة السيبرانية.

[206] *World Federation of Scientists- Combating cybercrime requires significant international cooperation and preventative measures, and this is especially important in deterring acts against critical infrastructure. Document WSIS-03/GENEVA/CONTR/6-E19 November 2003*

[207] *UN document A/RES/57/239, 31 January 2003, p. 2- the resolution calls for more awareness and responsibility by capable states to "act in a timely and cooperative manner to prevent, detect and respond to security incidents"*

[208] *Creation of a Global Culture of Cyber security and the Protection of Critical Information Infrastructures, UN document A/RES/58/199, 30 January 2004, p. 2. 95- the resolution invites all relevant international organizations and Member States "that have developed strategies to deal with cyber security and the protection of critical information infrastructures to share their best practices and measures that could assist other Member States in their efforts to facilitate the achievement of cyber security"*

ونذكر هنا، قرار اصدر في العام ١٩٩٠، حول قانون جرائم المعلوماتية[209]، ثم قرارا آخرا في العام اللاحق، حول مكافحة الاستخدام الجرمي لتقنيات المعلومات والاتصالات[210]. كما اصدرت الأمم المتحدة، قرارا خاصا حول الأمن السيبراني، في العام ٢٠٠٣[211]، ركز على القدرة على مكافحة الجريمة السيبرانية، ومن ثم اصدرت قرارا حول الموضوع نفسه، في العام ٢٠١٠، وملحقا حول ضرورة ان تلجأ الدول، إلى إجراء تقييم ذاتي بمحض ارادتها، لمعرفة مدى تناسب اطرها التشريعية، وقدرتها على مكافحة الجريمة السيبرانية، على ضوء التطورات السريعة الحاصلة، في مجال تقنيات المعلومات والاتصالات[212].

كذلك بذلت جهود عدة، من قبل مجموعات عمل متخصصة، بدعم من الاتحاد الدولي للاتصالات[213]، حيث برزت الحاجة إلى تعاون الدول فيما بينها، لاقرار مجموعة من المعايير والقواعد، التي تضمن الاستخدام الأمن للمجال السيبراني. وكانت روسيا، قد اعدت مسودة عدد من القرارات، وقدمتها إلى الأمم المتحدة، لإقرار اتفاقية سيبرانية. لكن هذه الاقتراحات لم تقر.

وتبقى هذه الجهود، كما المقررات والتوصيات، سواء منها تلك التي صدرت عن القمة العالمية، أو عن المنتديات الدولية لحوكمة الانترنت، وبالرغم من قيمتها السياسية والإعلامية، على المستوى الدولي، غير كافية، ولا فاعلة، نظرا لعدم الزاميتها القانونية، ولعدم اتاحتها امكانات العقاب، في حال مخالفتها. هذا عدا عن الهوة الرقمية، التي ما زالت تزداد اتساعا، بين الدول، والتي تمنع توقع باهتمام الدول المحدودة الإمكانات والقدرات، بالحفاظ على أمن الفضاء السيبراني، وبناء الثقة فيه، على ما جاء في مقررات وتوصيات تونس[214]. من هنا يبدو التعاون ضروريا، وملحا، بين الدول المتقدمة، وتلك التي تعاني من تخلف على مستوى التقنيات، والقدرات، والخبرات، وذلك منعا لاستغلال المجرمين للثغرات العديدة القائمة، والحؤول دون اقامة الجريمة المنظمة لشبكاتها الخاصة بتبييض الأموال، واعمال الخداع والغش المصرفي، في بلاد تعتمد تشريعات غير فاعلة، أو لا تعتمد إطلاقا اي تشريع، في مجال مكافحة الجريمة السيبرانية، مثل روسيا، والعديد من البلاد الافريقية.

وعليه، يبدو التوصل إلى إقرار نظام عالمي، اليوم وفي المستقبل القريب، بعيد المنال. فكيف يمكن لجميع دول العالم، وان اتفقت في إطار الأمم المتحدة على مكافحة الجريمة السيبرانية، ان تتفق على تحديد واحد للاعمال السيبرانية الشرعية، وغير الشرعية، سواء منها تلك التي تقوم بها الدول، أم تلك التي يقوم بها الأفراد؟ وكيف سيتم الاتفاق على مرجعية لحل الخلافات، وما هي آلية فرض قراراتها، لاسيما على الدول المارقة أو المخالفة؟

[209] *The UN GA resolution 55/63 dealing with computer crime legislation 1990*
[210] *In 2000 the UN GA resolution 56/121 on combating the criminal misuse of information technology*
[211] *In 2003 resolution (A/RES/57/239)*
[212] *A/RES/64/211*
[213] *Toward a universal Order of cyberspace: managing threats from cybercrime to cyber war. Permanent monitoring panel of cyber security- document wsis-2003- Geneva- www.itu.int*
[214] الوثيقةWSIS-II/TUNIS/DOC/6(Rev.1)-A182005نوفمبر
نحن نسعى إلى بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات من خلال تعزيز أسس هذه الثقة. ونحن نؤكد من جديد ضرورة المضي، بالتعاون مع جميع أصحاب المصلحة، في تعزيز وتنمية وتنفيذ ثقافة عالمية للأمن السبراني، كما ورد في قرار الجمعية العامة للأمم المتحدة 57/239، وفي قرارات بعض المحافل الإقليمية ذات الصلة. وتتطلب هذه الثقافة إجراءات وطنية ومزيداً من التعاون الدولي لتعزيز الأمن، والعمل في الوقت ذاته على النهوض بحماية المعلومات الشخصية وحماية الخصوصية والبيانات. وينبغي أن يعزِّز استمرار تنمية ثقافة الأمن السبراني إمكانيات النفاذ والتجارة، وأن يراعي مستوى التنمية الاجتماعية والاقتصادية في كل بلد وأن يحترم الجوانب الموجهة نحو التنمية في مجتمع المعلومات

٥. المبادرات الفردية

تعتبر المبادرات التشريعية الأميركية، حول الأمن السيبراني، من اهم المبادرات في العالم، بالرغم من المبادرات الوطنية والإقليمية والعالمية، التي تعالج هذا الامر. ذلك، انها ارتبطت مباشرة بمحاربة الإرهاب. ويعتبر الاتحاد الدولي للاتصالات، من اهم المنظمات الناشطة على هذا المستوى، عبر الاطر، والهندسيات، والمقاييس التي اقرها، ومن بينها X.509، التي تشكل أساس البنية التحتية للمفاتيح العامة، في التوقيع الإلكتروني[215]، المستخدم في البروتوكول التشعبي لنقل البيانات (HTTPS)، كما عبر انتقاله إلى وضع أجندة الأمن السيبراني العالمي، والتي تجاوز فيها الجوانب التقنية للأمن السيبراني، إلى السياسات، والتعاون، والتشريع، وبناء القدرات. لكن هذا لا يحجب بالطبع، وجود العديد من المبادرات التشريعية الوطنية والإقليمية، التي تعنى بالأمن السيبراني.

في لبنان، وبعد الجهود العديدة، للمرصد العربي للسلامة والأمن في الفضاء السيبراني، الذي اسسته الجمعية اللبنانية لتكنولوجيا المعلومات، انشئت لجنة خاصة، للتعامل مع قضايا الأمن السيبراني، حيث اكتشفت الحكومة اللبنانية ان مواقعها، هي الأضعف عالميا، على مستوى البرمجة والحماية. وقد تم الاكتشاف، أو الإقرار، بنتيجة القرصنة، التي قامت بها مجموعة مجهولة، لعدد من المواقع اللبنانية والحكومية، مثل موقع الأمن العام وموقع وزارة الخارجية والمغتربين وموقع وزارة الاقتصاد، واضعة صورة على الصفحة الرئيسة توحي بأن الشعب الفقير والجائع يطعم الحكومة المتخمة.

وقد ورد في هذا الإطار، شبه إعلان من الحكومة، بان معظم المُبرمجين اللبنانيين ومطوّري المواقع لا يهتمون للحماية، بسبب ضعف خلفيتهم في مجال الاختراق، الأمر الذي يجعل اللبنانيين يملكون معلومات ضعيفة عن الحماية، والاختراق، وبحيث أنّ ٧٠ في المئة من المواقع اللبنانية، مصابة بثغرات أمنية خطيرة جداً يسهل استغلالها من القراصنة.

ونقلا عما نشر من مقررات صادرة عن الحكومة، ننقل: «وعلى هذا الأساس، وبناء على المرسوم الرقم ٥٨١٨ تاريخ ٢٠١٢/٦/١٣، وحيث أن أمن المواقع الإلكترونية وأمانها هما مسؤولية مشتركة تقع على عاتق الإدارات المعنية كلها، للحفاظ على المصلحة العامة وانتظام سير العمل فيها وضمان أمن المواقع الإلكترونية ومحتواها وحمايتها من أعمال القرصنة، التي قد تلحق ضرراً فادحاً بالقطاع العام، قرّر مجلس الوزراء، في ٢٥ تموز الماضي، الموافقة على تشكيل لجنة أمنية وطنية لوضع توصيات أمنية لاستضافة المواقع الحكومية على شبكة الإنترنت».

وقد اوكلت بموجب المرسوم الذي صدر عقب ذلك، وحمل الرقم ٥٨١٨ تاريخ ٢٠١٢/٦/١٣، مهمة حماية الفضاء السيبراني، ومواقع الحكومة، إلى لجنة اختير أعضاؤها، من ممثلين عن الإدارات العامة، والأجهزة الأمنية، والجهات المصرفية. واسندت إليها المهمات التالية:

١. وضع سياسة أمنية للفضاء السيبراني، والمواقع الحكومية الإلكترونية.

[215] *UN ITU-T X.1205 —Overview of Cyber-security : 2Cyber-security has been defined by the ITU to mean —the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.*

٢. وضع التوصيات واقتراح التعاميم في هذا الإطار، ومتابعة مسألة تطبيقها في الإدارات العامة والمؤسسات العامة.

٣. تنسيق العمل على المستوى الوطني، في مجال الأمن السيبراني، والعمل على مستوى التوعية، والخدمات الاستباقية، ومواجهة الخروق السيبرانية، والجرائم المعلوماتية، ودعم الجهود لمعالجتها.

٤. اقتراح الخطوات العملية وتقديم التوصيات الضرورية لإنشاء مركز وطني للأمن السيبراني.

على المستوى الدولي، وضعت مجموعة الثماني، عددا من المبادرات في هذا المجال، ركزت بشكل خاص على التعاون بين الدول، من خلال شبكة مراكز متخصصة، أطلق عليها اسم: ٧/٢٤، تؤمن التواصل بين الأجهزة الأمنية، المعنية بتطبيق القانون والملاحقة. وتتولى هذه المراكز، إضافة إلى اعمال الحماية، التدريب والتأهيل، وتطوير الاطر التشريعية المناسبة لتامين السلامة والأمن، ومحاربة الجريمة الإلكترونية، وتشجيع التعاون بين الأجهزة الأمنية المعنية، وقطاع الاتصالات التجاري.

كذلك اصدرت الجمعية العامة للامم المتحدة، عددا من القرارات، وذلك في إطار التنمية في مجال الاتصالات والمعلومات، في مجال الأمن السيبراني العالمي، ومن اهمها: ٥٣/٧٠، في العام ١٩٩٨، و ٥٤/٤٩ في العام ١٩٩٩، و ٥٥/٢٨ عام ٢٠٠٠، و ٥٦/١٩ عام ٢٠٠١، و ٥٨/١٩٩ عام ٢٠٠٣.

كما دعت الجمعية العامة إلى تكوين فريق من الخبراء، لدراسة امكانات إيجاد قواسم مشتركة، بين دول العالم، تضمن الحفاظ على الأمن السيبراني[216]. الا ان هذا الفريق فشل في التوصل إلى تفاهم، في العام ٢٠٠٤، فاعيد تكوين فريق عمل ثان، في العام ٢٠٠٩، واوكلت اليه مهمة متابعة دراسة المخاطر السيبرانية الجسيمة، وامكانات وضع تدابير تضمن التعاون في مواجهتها. وقد اصدر، بعد عام على تكليفه، تقريرا[217] دعا إلى مزيد من الحوار بين الدول، لمناقشة المعايير المتعلقة باستخدام الدول لتقنيات المعلومات والاتصالات، بهدف الحد من المخاطر الجماعية، وحماية البنية الحرجة الوطنية، والبنية التحتية الدولية. كما اوصى، ببناء الثقة، واعتماد تدابير لدعم الاستقرار، لمعالجة آثار استخدام الدول لتقنيات المعلومات والاتصالات، بما في ذلك تبادل وجهات النظر، حول استخدام الدول لهذه التقنيات في النزاعات.

وقد تمكن من وضع أجندة عمل، للعمل المستقبلي، تضمنت سلسلة من الإجراءات التي يمكن للدول اتخاذها، لتعزيز الشفافية، والثقة فيما بينها، بما يسمح باستشعار الأخطار، ومنعها، ومعالجة آثارها، والحد منها، عبر شبكة اتصالات بين الدول، وبما يحد من امكانات التصعيد والنزاعات العسكرية. وقد برزت في التقرير، إجراءات تعزيز الشفافية والثقة، على النحو التالي:

- تبادل المعلومات ووجهات النظر، حول السياسات الوطنية وأفضل الممارسات، وآليات اتخاذ القرار، والمؤسسات الوطنية الخاصة بتعزيز الأمن السيبراني. وكانت الولايات المتحدة والمانيا، قد تبادلتا دراسات حول الدفاع السيبراني مع روسيا، خلال العامين ٢٠١٢ و٢٠١٣.

[216] *The General Assembly, in its resolution 57/53, of 22 November, on the subject, called upon Member States to promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field, consistent with the need to preserve the free flow of information; considered that the purpose of such measures could be served through the examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems, and reiterated its request to the Secretary-General, already contained in its resolution 56/19, to carry out a study on these concepts, with the assistance of a group of governmental experts, to be established in 2004.*

[217] *UN document A/65/201, 30 July 2010*

في المقابل، وفي مسودة حول «قواعد السلوك في المجال السيبراني الخاصة بالدول، قدمت ضمن تقرير، الى الامين العام للامم المتحدة في العام ٢٠١١، اقترحت فيها روسيا والصين، منع «اسلحة المعلومات» "information weapons"، وتطوير تقنياتها، لتعودا وتقران خلال اعداد تقرير الخبراء، بعدم ضرورة هذا المنع، كون التقنيات التي تطور، تقنيات ذات استخدامات مزدوجة: ايجابية وسلبية. ويشكل هذا الامر، انضماما الى الآراء السائدة، التي اقرت مقاربة تقول بضرورة البدء بإجراءات بناء الثقة التقليدية، واسس التعاون، قبل منع ما لا يمكن التأكد من طبيعته. كما دعا التقرير الى بناء بيئة معلوماتية سلمية، على غرار ما هو معمول به، في قانون استخدام الفضاء الخارجي، ومعاهدات النقل الجوي، وغيرها من المجالات، التي يمكن ان تؤثر على السلم الدولي.

وفي العام ٢٠١٢، اعيد تكوين هذا الفريق، لمتابعة المهمة، انطلاقا من التقرير الصادر في العام ٢٠١٠، حيث قدم تقريرا، أوصى بارساء حوار منتظم بين المؤسسات، والمنظمات، والدول، في إشارة منه إلى ضرورة ان يشمل التعاون، أكبر عدد ممكن من الشرائح المعنية بمجتمع المعلومات، بما فيها المجتمع المدني، ومجال الأعمال، والقطاع الخاص. الا ان هذا التفاهم، لم يحسم الخلاف، حول دور الأمم المتحدة في النقاشات الدائرة حول النشاطات السيبرانية، والتي يمكنها ان تهدد السلم والأمن الدوليين.

في العام ٢٠١٣، اصدرت الهيئة العامة بالاجماع، قراراً[218]، أخذت به علما بنتائج عمل الفريق، خلال العام ٢٠١٢–٢٠١٣، وطلبت من الامين العام، اعادة تكوين فريق جديد. وتألف هذا الأخير من عشرين عضوا [219]، وعقد اربعة اجتماعات، ليقدم تقريرا يستكمل ما بدء به من عمل، حول بناء الثقة، والشفافية، ومسؤولية الدول، والتعاون، وبناء القدرات، في الفضاء السيبراني. كما ناقش التقرير كيفية تطبيق القانون الدولي، على استخدام تقنيات المعلومات والاتصالات، وأصدر توصيات للعمل المستقبلي، جاء فيها:

- ضرورة مراعاة الدول لمبادئ القانون الدولي، ولاسيما منها سيادة الدول، وحل النزاعات بالطرق السلمية، وعدم التدخل في الامور الداخلية للبلدان الاخرى.
- التزام الدول في الفضاء السيبراني، باحترام موجباتها التي يقرها القانون الدولي، بما يتناسب مع احترام وحماية حقوق الإنسان والحريات الأساسية.
- امتناع الدول عن استخدام البروكسيز Proxies، لارتكاب اعمال غير شرعية، والحرص على عدم استخدام اراضيها من قبل جهات غير حكومية، لارتكاب افعال مماثلة.
- على الأمم المتحدة ان تلعب دورا قياديا، في تعزيز الحوار حول سلامة استخدام تقنيات المعلومات والاتصالات، من قبل الدول، وفي تطوير فهم مشترك لكيفية تطبيق قواعد القانون الدولي، واصول ومبادئ التصرف المسؤول للدولة.

وقد طلبت الجمعية العامة، تكوين فريق آخر، من المتوقع أن يقدم تقريره، في العام ٢٠١٧.

[218] *UN General Assembly resolution 68/243*
[219] *Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Russian Federation, Spain, United Kingdom and United States of America.*

٦. الجهود العربية

أ- غياب أطر قانونية واضحة وشاملة

تنتشر الجرائم السيبرانية في المنطقة العربية، كما تنتشر في بقية أجزاء العالم، وذلك، في غياب أطر قانونية واضحة وشاملة، تضمن مكافحة فاعلة لها. فالتشريعات العربية السيبرانية المتوافرة، تركز بشكل أساسي، على مكافحة الجرائم، التي تتصل بحماية التعاملات الإلكترونية، والتجارة الإلكترونية، تاركة فراغا تشريعيا واضحا، على مستوى مكافحة الجريمة السيبرانية، في المجالات الاخرى. فقد بادرت العديد من الدول العربية، إلى إقرار تشريعات لمكافحة الجريمة السيبرانية[220]، بينما بقي البعض الآخر دون تشريع. يضاف إلى ذلك، اللجوء إلى تطبيق قواعد القانون الجزائي، في بعض البلدان، التي لا تملك تشريعا سيبرانيا، وذلك بالرغم من ان بعضها لم يعدل هذه القوانين لتشمل الجرائم السيبرانية، ما يضمن ملاذا آمنا لها.

وفي سياق متصل، يسجل تعاون بين بعض البلدان العربية، من خلال الفرق الوطنية للاستجابة للحوادث ولطوارئ الانترنت، حيث اطلقت مبادرتان إقليميتان: الأولى مبادرة مجلس التعاون الخليجي، (GCC-CERT) حيث تتعاون عُمان، والإمارات العربية المتحدة، وقطر، والكويت، والمملكة العربية السعودية والبحرين، أما الثانية، فهي مبادرة منظمة التعاون الإسلامي (OIC) حيث تتعاون البلدان الأعضاء، عبر الفرق الوطنية المعنية بأمن الحاسوب، والاستجابة للحوادث الحاسوبية (CSIRT) والفرق الوطنية للاستجابة للطوارئ الحاسوبية (CERT) في البلدان الأعضاء، وفريق الاستجابة للطوارئ الحاسوبي التابع للمنظمة. (OIC-CERT).

ويشار في هذا المجال، إلى تعاون الدول العربية، سواء في إطار جامعة الدول العربية، أو في إطار اتفاقيات ثنائية، في عدد من المجالات، التي يمكن ان تفعل للتطبيق في الفضاء السيبراني، والتي يمكن ان تعتبر إطارا مسهلا للتعاون، مثل: الاعتراف بتنفيذ التبليغات والانابات القضائية، تنفيذ الاحكام القضائية الصادرة بصيغة نهائية، سواء منها تلك المقررة لحقوق مدنية، أو تجارية، أو تلك القاضية بتعويضات، تسليم المجرمين، ومكافحة الإرهاب.

ب- مبادرة مركز البحوث والدراسات القانونية والقضائية

ووعيا منه لخطورة المسألة، وفي إطار سعيه الدائم لمواكبة التطورات المتسارعة، لاسيما في مجالات التواصل العربي والتنسيق والتكامل البيني، عمل المركز العربي للبحوث القانونية والقضائية في جامعة الدول العربية، على وضع مشروع اتفاقية عربية لضمان أمن وسلامة الفضاء السيبراني. وبالفعل، فقد تمت مناقشة هذا المشروع، خلال اجتماعات عقدها المركز، وشارك فيها نخبة من الخبراء والمختصين القانونيين والتقنين العرب، الموفدين من حكوماتهم. وقد شارك في هذه النقاشات، أعضاء المرصد العربي للسلامة والأمن في الفضاء السيبراني.

[220] في مصر: القانون ١٢٠ لسنة ٢٠٠٨ ،قانون الطفل المصري بالتعديل الصادرعام ٢٠٠٨ ، قانون الملكية الفكرية رقم ٨٢ لسنة ٢٠٠٢، قانون الاتصالات رقم ١٠ لسنة ٢٠٠٣ قانون التوقيع الالكتروني رقم ١٥ لسنة ٢٠٠٤، قانون المحاكم الاقتصادية رقم ١٢٠ لسنة ٢٠٠٨

وقد عمم المركز هذا المشروع، على الدول العربية، من خلال وزارات العدل فيها، وهو بانتظار ملاحظاتها، لعرضها على مجلس وزراء العدل العرب، لاعتمادها وإقرارها، تمهيدا لاتخاذ الخطوات التنفيذية المناسبة، في هذا المجال، في كل دولة عربية.

أبرز عنوان المشروع "بناء الثقة في الفضاء السيبراني"، الهدف الأساس من الاتفاقية، وهو الالتزام برفاه الدول وشعوبها، وبتسخير طاقات تقنيات المعلومات والاتصالات، لخدمة النمو والتطوير الإنساني. وقد ركزت الديباجة، على اهمية مواكبة متطلبات حماية أمن المجتمعات العربية، في العصر الرقمي، من خلال التعاون بين الحكومات العربية، وإقرارها للاطر التشريعية والتنظيمية الملائمة والمنسجمة، التي تضمن تبادل المعلومات، بين الأجهزة المعنية، وتضافر جهود السلطات القضائية، لمكافحة الجريمة السيبرانية.

بني مشروع الاتفاقية، على الالتزام بالمبادئ الاخلاقية والدينية السامية، وبالخصوصية الثقافية العربية، واحترام مبادئ القانون الدولي، والمواثيق. كما وضع إطار لما يمكن الاتفاق عليه، من تجريم لبعض الأعمال غير الشرعية، لاسيما منها، تلك الخاصة بالمحتوى. فلهذه الأخيرة، ارتباط وثيق بطبيعة المجتمع وثقافته، التي تؤثر بشكل أكيد، على الوصول إلى تفاهم حول التجريم المزدوج، لبعض الجرائم، التي يمكن الا تعتبر كذلك، في مجتمعات اخرى، لاسيما ما يرتبط منها بالسمات الثقافية للمجتمع.

وقد لحظت مبادئ الاتفاقية، الإقرار بحق سيادة الدول على اقاليمها، وبموجب التزامها حماية الفضاء السيبراني، بما يمنع تحويله إلى مجال للنزاعات، سواء منها في ذلك، تلك التي يرتكبها الأفراد، أو التي تتغاضى عن ردعها الدول، أو تلك التي ترتكبها. كما لحظت، مبدأ الامتناع عن استخدام تقنيات المعلومات والاتصالات، في الاعتداء على دولة اخرى، أو تسهيل هذا الاعتداء. يضاف إلى ذلك، موجب الالتزام بتسخير سياسات الدول ومواردها في المجال السيبراني، للتعاون على حماية الأمن القومي العربي، ومنع تحول الفضاء السيبراني، إلى مركز انطلاق عمليات عسكرية، أو إستخباراتية، أو تخريبية، أو إرهابية، ليس فقط ضد الدول الأعضاء، وانما أيضا ضد دول العالم الاخرى.

أما مضمون المشروع، فقد توزع تحت عناوين، يمكن اعتبارها العناصر الأساسية والركائز الضرورية، لمكافحة الجريمة السيبرانية، انطلاقا من خصوصية طبيعة الفضاء السيبراني، العابرة للحدود، التقنية، والمتحركة. ونذكر منها على سبيل المثال:

- تجريم كل اشكال الاعتداء على الشبكة العالمية للمعلومات والأنظمة، أوعلى الأشخاص أو الأموال، باستخدام تقنيات المعلومات والاتصالات.
- التعاون في المجال الأمني
- التعاون بين السلطات القضائية
- اعداد البنية التحتية الضرورية لتامين فعالية الجهود
- إنشاء مرجعية خاصة تؤمن التنسيق والتعاون بين الدول الأعضاء، تحت مسمى: "المنظمة العربية لحماية الفضاء السيبراني"
- تعزيز القدرات وبنائها وتبادل الخبرات

- اعتماد سياسات واستراتيجيات وطنية، تشكل ارضية التعاون ومرتكزه
- إنشاء مراكز استجابة لطوارئ الانترنت، وبناء شبكة علاقات بينها

٧. مدى كفاية الاتفاقيات الإقليمية

شملت الاتفاقية الأوروبية، جرائم اختراق الأنظمة المعلوماتية، والتزوير والاحتيال، والاعتداء على الملكية الفكرية، الا انها تركت جانبا، عددا من التصرفات غير الشرعية، التي لا تقل خطرا على استقرار الأمن والسلامة في الفضاء السيبراني، مثل سرقة الهوية، والبريد غير المرغوب فيه، والترصد، والإرهاب الإلكتروني. لذلك، وضع بروتوكول ملحق لها، وعدد من الاتفاقيات، التي ترعى اشكالا اخرى من الاستخدامات الجرمية.

كذلك لم تلحظ هذه الاتفاقية، امكانية الوصول إلى البيانات، عبر اتصال مباشر بمقدم خدمات الانترنت، سواء منها تلك الخاصة بالمحتوى، أو بالاتصال، دون المرور بالجهات الرسمية القانونية، في البلدين. ذلك انها تركز، على موافقة صاحب الحق في افشاء المعلومات، وعلى فرضية علم طالب البيانات بمكان وجودها الفعلي، في وقت الارسال أو التلقي. وهنا يبرز خطر الاعاقة، التي يسببها اللجوء إلى القنوات الرسمية التقليدية، في التعاون في المجال الجزائي، بما يعنيه من بطء، لا يتناسب وسرعة الحركة، في المجال السيبراني.

فلجوء الدول إلى تطبيق مبدأ التعامل بالمثل، في حال عدم الاستجابة إلى طلب الدول التي لا تعتمد قوانين منسجمة لمكافحة الجريمة السيبرانية، أو لمكافحة هذا المحتوى المسيئ أو غير الشرعي، يعني المرور بالقنوات الدبلوماسية والقانونية التقليدية للتعاون، التي لا تلحظ، لا طبيعة الجريمة السيبرانية، ولا ادلتها، عند الحاجة إلى ذلك، ما يعرقل التحقيقات، ويطيل عمر القضية، ويذهب بالأدلة ويزيلها.

أمام هذا الواقع، تبقى الحاجة قائمة إلى مقاربة دولية، لاسيما على مستوى الملاحقة والمكافحة، وبشكل خاص، فيما يتعلق بجمع الأدلة والاثبات. وغني عن القول، ما للاثبات من اهمية في التجريم، وتفعيل آليات المحاسبة، تعزيزا للقدرة على الردع.

كذلك، لا بد من إقرار مقاربة منسجمة، لآليات نقل البيانات خارج الحدود، تسمح للدول التي تعتمد حماية البيانات، وتعتبرها موجبا قانونيا، بان تتبادلها، مع الدول التي تحتاج اليها. وكانت مسودة الاتفاقية الافريقية لمكافحة الجريمة السيبرانية، قد تنبهت إلى هذا النقص[221]، فاوردت بعض البنود، التي تلحظ ما يمكن ان يدعم، فاعلية التبادل والتعاون.

---

[221] *Draft African union convention on the establishment of a legal framework conducive to cyber security in Africa or draft African union convention on the confidence and security in cyberspace. http://au.int/en/sites/default/files/AU%20Convention%20EN.%20(3-9-2012)%20clean_0.pdf*

Article III – 54- *Each Member State of the African Union have to take necessary legislative measures to ensure that the violation of the secrets stored in a computer system attracts same punishments applicable to the offense of violation of professional secrets.*

Article III – 55 - *Each Member State of the African Union have to take necessary legislative measures to ensure that, where the imperatives of the information so dictate, the investigating judge can use appropriate technical means to gather or register in real time the data in respect of the content of specific communications in its territory, transmitted by means of a computer system or compel a service supplier to gather and register the data within the framework of his/her technical capacities, using the existing technical facilities in its territory or that of States parties, or provide support and assistance to the competent authorities towards the gathering or registration of the said computerized data.*

في كل الاحوال، لقد أصبح أكيدا، نتيجة تراكم التجارب المختلفة، أن التعاون الإقليمي والدولي، شديدا الأهمية، للتمكين من تبادل المعلومات والخبرات، التي تسمح للبلدان، بمواكبة عبور الجريمة لحدود سيادتها، سواء لدى انطلاقها من أراضيها، أو لدى استهدافها لهذه الاراضي، من داخل اراضي دولة اخرى.

ولقد أتاح التعاون في المجال القانوني، بشكل عام، تحديد الجرائم موضوع المكافحة، والتدابير الإجرائية، والأدلة، والاختصاص القضائي، وتحديد المسؤوليات، وآليات التعاون، حيث اعتمد مثلا، على توصيف لعدد من الجرائم، وعلى تسليم المجرمين، لاسيما في تلك التي اتفق على كونها، جرائم تهدد الإنسانية، والاستقرار الدولي والاقتصادي، مثل الاتجار بالرقيق، وتبييض الأموال، والاتجار غير الشرعي بالمخدرات والأسلحة. وأقرت القوانين الجزائية، صلاحيات قضائية، بنيت على مبدأ سيادة الدول على اقاليمها، ترتكز إلى مكان ارتكاب الجرم، أو مكان ظهور نتائجه، أو جنسية الشخص الذي وقعت عليه الجريمة.

وللتعاون الناجح، آليات تعاون تنفيذية ثنائية وجماعية، وتنسيق يضمن تنظيم أشكال التعاون وتحفزيه، وانسجاما مع التحديات المرتبطة. وعليه، لا بد لقياس كفاية اية اتفاقية، من النظر، ليس فقط إلى مضمون الاتفاقية بحد ذاته، وانما أيضا إلى ما يقر من آليات، ويتخذ من إجراءات، لضمان تنفيذ هذا الاتفاق.

فلقد اظهر العديد من الدراسات الميدانية، في البلدان التي اقرت تشريعات وطنية، واتفاقات إقليمية لمكافحة الجريمة السيبرانية، فعالية الاطر التنظيمية والتشريعية، في ملاحقة الجريمة السيبرانية، وتفكيك الشبكات الإجرامية المنظمة، والمنتشرة في عدد من البلدان المختلفة، لاسيما فيما يتعلق بمنع استخدام الأطفال في انتاج المحتوى الجنسي، وتوزيع المواد الجنسية التي يستغلون فيها. كذلك، نجح هذا التعاون، في مكافحة جرائم خاصة بتوزيع المخدرات، والادوية غير الشرعية، والإرهاب.

لكن، وبالرغم من اقتناع الجميع، باهمية الوصول إلى هذا الانسجام، على مستوى التجريم، لاسيما في الجرائم الخاصة بالمحتوى، يبقى ان المسائل التي يمكن الوصول إلى اتفاق حولها في هذا المجال، على المستويين الدولي والإقليمي، تظل محدودة، ليس بسبب اختلاف المفاهيم والأنظمة القانونية، فحسب، بل وبسبب العوامل الثقافية والاجتماعية المختلفة أيضا.

وهنا لا بد من الانتباه، إلى اختلاف التعامل مع هذا النوع من الجرائم، نظرا لكونه أكثر تعقيدا، لاسيما على ضوء اختلاف الأنظمة القانونية، التي يمكن ان تعتبر عملا، أو محتوى معينا، مخالفا للقانون، فيما لا تعتبره الأنظمة الاخرى كذلك، وذلك في الوقت نفسه.

والملاحظ في هذا المجال، اهتمام الولايات المتحدة الأميركية، بشكل خاص، بمصالحها، أكثر من اهتمامها بالتعاون والتنسيق مع الدول الأخرى، لإيجاد الحلول لتهديدات الجريمة السيبرانية. فبعد موافقتها على الاتفاقية وبروتوكولاتها اللاحقة، اعترضت في العام ٢٠٠٢ على تعديل ادان نشر مواد عنصرية، أو محرضة على كراهية الاجانب، بواسطة الأنظمة المعلوماتية، إضافة إلى الاهانات، والتحقير، وتأييد المجازر والجرائم ضد الإنسانية، متذرعة بتعارض هذا التعديل، مع حرية التعبير، المكرسة في الدستور الأميركي. على خط مواز، وبالرغم من الحملة الأميركية على الإرهاب، يلاحظ وجود عدد من المواقع، في الولايات المتحدة الأميركية، للحركات المصنفة إرهابية من قبل الإدارة ك"حماس".

٨. نظام عالمي للمكافحة

بناء على ما تقدم، يبدو واضحا، ان أفضل الطرق لمكافحة الجريمة السيبرانية، هي إقرار نظام عالمي، يرتكز إلى تعاون بين مختلف دول العالم، التي تعمل معا في إطار سياسة موحدة، وإطار تشريعي وتنظيمي منسجم. الا اننا نلاحظ، من واقع الحال، ان المنظمات الدولية، كما الحكومات المختلفة، لم تنجح في اقناع الجميع، بذلك. وبالتالي، فما زال المجرمون السيبرانيون، يعملون على استغلال نقاط الضعف، والثغرات التشريعية الوطنية والإقليمية والدولية، حيث لم تنجح محاولات إيجاد الإطار الفاعل والمتناسق، إلى الآن.

فالدول العربية، كما الجامعة العربية، لديها القدرة الكافية، على الاستجابة لتحديات التشريع في الفضاء السيبراني، دون وصاية أو توصية، من أية جهة كانت وفقد اقرت جامعة الدول العربية، قانونا نموذجيا لمكافحة جرائم تقنية المعلومات، وتعمل حاليا، كما أسلفنا، على اعداد مسودة اتفاقية عربية، لحماية الأمن في المجال السيبراني.

من هنا، يبقى المجال السيبراني، وبالرغم من تعدد المبادرات التشريعية، والتوصيات، والاتفاقات الإقليمية، بحاجة إلى اتفاق دولي على معايير، ومقاييس، وقواعد قانونية، تمنع بروز جنات للجريمة، وتضمن سلامة الممتلكات والأشخاص والمجتمعات، كما تضمن استقرار العلاقات بين الدول والأفراد. فالتقنيات في تطور مضطرد، وسريع، والخشية تتصاعد من استفحال آثار الأعمال الجرمية، على نحو تصعب معه السيطرة عليها.

لذا، لا بد من العمل، على ان تشكل الاتفاقيات الإقليمية، إطارا يعزز ارساء الانسجام، بين مندرجات ومقاربات الاتفاقيات الخاصة بالتعاون في مجال مكافحة الجريمة السيبرانية، بحيث يبنى على التجارب السابقة، ويستفاد منها، وبحيث تلحظ بنود تضمن فاعلية التعاون، مثل:

- التزام السلطات المعنية، بالرد ضمن وقت محدد
- الالتزام بمراجعات دورية، وتقيمية، لقياس قدرة التشريعات الوطنية، على الاستجابة لمتطلبات المكافحة، من جهة، وللمستجدات التقنية وتحديات التعاون الإقليمي والدولي، من جهة اخرى
- تبادل الحق في الولوج المباشر، إلى الأنظمة المعلوماتية، الموجودة خارج الاراضي الوطنية، ضمن اطر تشريعية تضمن الحقوق والحريات، والأمن القومي
- تحديد نقاط اتصال ثابتة، لتنسيق التعاون بين السلطات القضائية، المعنية بالبحث والتحقيق
- تمكين التعاون، وتثبيت آليات وممارسات فضلى، في هذا المجال
- ادراج التدريب والتأهيل، في اطر التعاون الإقليمي والدولي، لاسيما وان العديد من الدول، تقر بمحدودية قدراتها، على مستوى الملاحقة والمكافحة[222].
- إنشاء مراكز وطنية لمكافحة الهجمات السيبرانية، في البلدان التي لم تبادر بعد، إلى ذلك.

[222] *Comprehensive Study on Cybercrime Draft - February- 2013 – executive summary- xviii. Two-thirds of countries view their systems of police statistics as insufficient for recording cybercrime. Police-recorded cybercrime rates are associated with levels of country development and specialized police capacity, rather than underlying crime rates*

- تركيز أكثر، على التزام الأعضاء بسياسات التوعية، لاسيما وان الحلقة الأضعف في موضوع الأمن والسلامة، هي مستخدم الانترنت، فما بالك إذا كان هذا المستخدم، طفلا أو مراهقا، لا يعي وجود أشخاص يتربصون به، ويستهدفون البيانات الشخصية التي تعود اليه، والى أفراد اسرته؟
- اعتماد أسس للتعاون، بين مختلف اصحاب المصلحة، كالشركات والمؤسسات المالية، والمجتمع المدني، والدولة، لمواجهة الثغرات ونقاط الضعف، في البرامج والتطبيقات التي تعتمد، في تقديم الخدمات الاجتماعية، والصحية، والمالية، والادارية، بما يعزز أمن مجتمع المعلومات.

وضع استراتيجيات وسياسات وطنية، تلحظ التعاون وآليات تفعيله، على المستويات كافة، الداخلية بين أصحاب المصلحة المتعددين، والإقليمية بين الدول ذات المصالح المشتركة، والدولية مع دول العالم الاخرى.

﴿ الفصل الثامن ﴾

البيانات الشخصية: بين الرقابة وصون الحريات

١. بين الاخفاء والخوف

"إذا لم يكن لديك شيء تخفيه، فليس لديك شيء تخافه"، شعار استخدمته الحكومة البريطانية، في سياق زرعها، كاميرات الرقابة في المدن والقرى، فهل هذه المقولة صحيحة؟

تكون هذه المقولة صحيحة، فيما لو كان لدينا استعداد، لكشف ميولنا، ورغباتنا، ومحيطنا العائلي، وأسماء اصدقائنا، ومحتوى مخابراتنا، واماكن تواجدنا، ونوعية مشترياتنا، وقيمة رصيدنا المالي، ومدخراتنا، وموقع منزلنا، ومحتويات غرف نومنا، لأي كان، وفي كل الاحوال والاوقات.

وقبل الموافقة على هذه المقولة، لا بد من تحديد ردة فعل أي شخص، ليس لديه شيء يخفيه، على غريب يقترب منه في الشارع، ويسأله عن رقم هاتفه، أو عنوانبيته، أو عن مقاس ثيابه، أو وزنه، أو حتى نوع سيارته.

وماذا لو سئل هذا الشخص، عن اسمه، واسم عائلته، ووالديه؟

أو ماذا لو سئل، عن الامكنة التي زارها خلال اليوم، أونوع الحساسية الذي يعاني منه، أو عن سوابقه المرضية، وحالته العصبية، وفئة دمه، وانتمائه السياسي، ومعتقداته الدينية؟

بعيدا عن القانون، ومن منظور اجتماعي بحت، يعتبر هذا النوع من الاسئلة، بنظر الكثيرين، من الامور الممجوجة، وغير المقبولة، واعتداء فاضح على الخصوصية، في المجتمعات الغربية، كما في المجتمعات الشرقية، على حد سواء، والا لماذا ينعت الناس بالفضول السلبي، وقلة الذوق، وغيرها من التعابير التي تطلق على من يقوم بهذه التصرفات. ولماذا تذهب بعض ردات الفعل، إلى التساؤل، عما إذا كان طارح الاسئلة، يعمل تحريا؟

إذا كان صحيحا، ان من لا يخفي شيئا، لا يخشى من انفضاح اي تفصيل خاص، فالصحيح أيضا، أن لكل شخص حياته الخاصة، التي لا يريد عرض تفاصيلها أمام العالم، كما لا يريد لهذا العالم، ان يتدخل في شؤونه. والصحيح أيضا، أنه وبالرغم من انتماء الفرد إلى مجتمع، فان للفرد حياة خاصة، وشخصية مميزة. ولذا، لحظت حرمة لمحيط الشخص، حيث تنتشر دلائل خصوصيته، كالبيت والمراسلات، ووضعت قواعد حماية، لا يجوز اختراقها، الا بموجب نص قانوني، وفي حال اعتداء هذا الشخص، على حقوق الآخرين، ومخالفته للقوانين المحددة، والمرعية الإجراء.

والصحيح أكثر، أن هذه المقولة، نوع من محاولة القضاء على الحق في الخصوصية، من خلال الايحاء، بان من يخشى على حماية بياناته الشخصية، لا بد وان يخفي أمرا مخالفا للقانون، أو أمرا سيئا.

فما هو الحق في الخصوصية؟ وما هي البيانات الشخصية؟ وكيف يمكن الاعتداء على هذا الحق في غياب حماية البيانات الشخصية؟ وما هي الصلة بين حماية البيانات الشخصية والحق في الخصوصية والأمن السيبراني؟ وما هو الإطار القانوني الذي يتم التعامل على أساسه مع المخاطر التي يتعرض لها هذا الحق؟

هذا ما سنحاول الإجابة عليه، من خلال العناوين الآتية.

٢. البيانات الشخصية

أ- تعريفات

يختلف العامة على ما يعتبر بيانات شخصية، أو بيانات حساسة، أو معلومات يتحفظون على نشرها. الا أن مقتضيات الأمن السيبراني، تفترض اعتماد قواعد واضحة، لما يعتبر بيانات شخصية، بغية وضع النصوص القانونية المناسبة، وتأمين الحد الادنى من الحماية المطلوبة.

ويمكن تعريف هذه البيانات، استنادا إلى القواعد الارشادية التي وضعتها منظمة التعاون الاقتصادي والتنمية، بانها "... كل معلومة عائدة لشخص طبيعي محدد أو قابل للتحديد"[223].

وعليه، فهي تلك البيانات، التي تنقل معلومات يمكن ربطها بشخص معين، لتحديد هويته.

الا أن هذا التعريف يثير بعض الإشكاليات، باعتباره قد استثنى بيانات، يمكنها ان تساعد على تحديد هوية الشخص، أو تعقبه وملاحقته، عبر تحديد مكان وجوده. وترد في هذا السياق، البيانات التي لا تعود إلى الشخص الطبيعي، وانما إلى وسيلة يستعملها: كرقم تسجيل السيارة، ورقم الهاتف الثابت والنقال، لاسيما متى بقيت خارج إطار التنظيم، الذي يستهدف حماية البيانات الشخصية. ويسمح هذا الاستبعاد، بالتعدي على خصوصية الأشخاص، دون رادع، نظرا لعدم امكانية تطبيق النص. وكان التشريع الفرنسي الذي صدر في العام ١٩٧٨، قد نص على حماية المعلومات الاسمية، حاصرا بذلك، نطاق تطبيقه بشكل دقيق، في كل معلومة تشير إلى هوية الشخص، من دون اي التباس. الا ان هذا القانون، جرى تعديله في العام [224]٢٠٠٤، ليصبح نطاق تطبيقه أكثر اتساعا، بحيث اعتمدت عبارة "المعلومات ذات الطابع الشخصي"، بما يمهد لحماية بيانات غير اسمية[225]، فاتحا بذلك المجال امام حماية أوسع، ولكن أمام التباسات أكبر.

وبالفعل، فقد اعترضت اللجنة الخاصة بالمعلوماتية والحريات في فرنسا، على الاجتهاد[226] الذي اعتبر في قرارين متتاليين صادرين عن محكمة الاستئناف في باريس، ان العنوان الخاص برقم التعريف

[223] *Lignes directives de l'OCDE . ..."toute information relative a une personne physique identifiee ou identifiable'.*
[224] *Loi 801 intitulee « loi pour la confiance dans l'économie numerique » du 21 juin 2004*
[225] *La loi du 6 janvier 1978 «informatique et libertés» visait les informations nominatives. La loi du 6 août 2004 remplace le terme «information nominative» par celui de «donnée à caractère personnelle»*
[226] *CA Paris, 27 Avril 2007 :" «L'adresse IP ne permet pas d'identifier le ou les personnes, qui ont utilisé cet ordinateur puisque seule l'autorité légitime pour poursuivre l'enquête (police ou gendarmerie) peut obtenir du fournisseur l'accès d'identité de l'utilisateur.». Et CA Paris, 15 Mai 2007 : » «Que cette série de chiffre en effet ne constitue en rien une donnée indirectement nominative relative à la personne dans la mesure où elle ne se rapporte qu'à une machine, et non à l'individu qui utilise l'ordinateur pour se livrer à la contrefaçon».*

الإلكتروني للجهاز IP[227] ، ليس من البيانات الشخصية، كونه يسمح بتحديد هوية جهاز، لا هوية الشخص الذي يستعمل الجهاز. وفي هذا، بحسب رأي اللجنة، خطر يفتح الباب للتعديات على الخصوصية، من خلال جمع هذه البيانات، من دون الحصول على ترخيص مسبق بذلك، كما هو مقرر لجمع البيانات الشخصية.

وفي لبنان، حدد مشروع القانون الذي اعدته وزارة الاقتصاد والتجارة [228]، البيانات الشخصية، على النحو الآتي: «يقصد بالبيانات ذات الطابع الشخصي، جميع أنواع المعلومات المتعلقة بشخص طبيعي، والتي تمكن من التعريف به، مباشرة أو غير مباشرة، بما في ذلك عن طريق مقارنة المعلومات المتعددة المصادر أو التقاطع بينها». ويبدو واضحا من هذا التعريف، ذي النطاق الواسع، استناده إلى قانون ٢٠٠٤ الفرنسي.

ولعل هذا التعريف الاوسع، هو ما يتناسب مع قانون كانت الغاية الأساسية منه، تعزيز الثقة في التجارة الإلكترونية، كما يدل عليه عنوانه. فتوفير مساحة أكبر للحماية، يعني معدلا أعلى من الثقة. بالإضافة إلى ذلك، يستجيب هذا التعريف، لحاجات العصر، في مواكبة التطورات المتسارعة، في مجال تقنيات المعلومات، حيث لم يعد ممكنا توقع قدرات تكنولوجيا معالجة المعلومات، ولا نتائج الجمع بين تقنيات مختلفة ومتنوعة، على الحياة الشخصية، وعلى أمن الدول.

ويعلو منسوب الأخطار، مع كشف بعض البيانات الشخصية، التي يمكن اعتبارها بيانات حساسة، وذلك، نظرا لما يمكن ان يتركه هذا الانكشاف، من أثر سلبي على كيفية التعامل مع المعني بها، سواء من قبل السلطات المختصة، أو من قبل الآخرين. وتتمثل هذه البيانات، في كل ما يكشف عن الآراء والمعتقدات، والوضع الاجتماعي، والميول السياسية والجنسية. من هنا، تكون القاعدة فيما يتعلق بهذه البيانات هي حظر معالجتها، والسماح بمعالجتها هو الاستثناء، وذلك في حالات محددة حصرا[229].

ب- قيمة ادارية واقتصادية

من الثابت، ان البيانات الشخصية مرتكز لبناء القرار الاداري والأمني، الهادف إلى إدارة الشأن العام، وتحقيق الاستقرار، ورفاه الشعب. من هنا، تعتبر البيانات الشخصية، مادة أساسية للعمل، في مختلف أجهزة الدولة، والقطاعات الأمنية، حيث تدار الاحوال الشخصية، والممتلكات العقارية، والاستثمارات، والشؤون الاجتماعية، والصحية، والتعليمية، والأمنية، بما يؤمن أمن المواطنين، ويحافظ على أمن الدولة.

---

[227] *L›adresse IP est le numéro qui permet d›identifier chaque ordinateur sur le réseau Internet. Elle se décompose dans version 4 en une série de 4 nombres allant de 0 à 255.*

[228] *ECOMLEB*

[229] *ECOMLEB- art. 20 « Il est interdit de collecter et de traiter des données à caractère personnel qui révèlent, directement ou indirectement, les opinions philosophiques ou politiques, l'appartenance syndicale ou confessionnelle, l'état de santé, l'identité génétique ou la vie sexuelle de la personne concernée. Toutefois, il est fait exception à cette interdiction de principe dans les cas suivants :*

1°- *Lorsque la personne concernée a rendu publiques lesdites données ou qu'elle consent expressément à leur traitement, à moins qu'une interdiction légale ne s'y oppose ;*

2°- *Lorsque le recueil et le traitement des données sont nécessaires à l'établissement d'un diagnostic médical ou à l'administration de soins par un membre d'une profession de santé ;*

3°- *Lorsque le recueil et le traitement des données sont nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;*

4°- *Lorsque des groupements sans but lucratif, à caractère philosophique, politique, syndical ou confessionnel tiennent, à leur usage exclusif, des registres de leurs membres ou correspondants non communicables à des tiers ;*

5°- *Lorsque des traitements justifiés par un intérêt public bénéficient des autorisations prévues à l'article 30 ci-après.*

ومن الثابت أيضا، أن هذه البيانات، قد تحولت إلى مرتكز للاقتصاد الرقمي، والى سلعة ذات قيمة اقتصادية، والى جزء من عناصر المؤسسات التجارية، بما جعل بيانات مستخدم الانترنت، الذي هو أي مواطن[230]، تتحول إلى مادة أولية، في تحقيق انتاجية الشركات المختلفة.

وبالفعل، تتهافت الشركات الخاصة، الناشطة على الانترنت، وفي مجالات الاتصالات كافة، على جمع البيانات الشخصية، ومعالجتها، واستخدامها، في عمليات الترويج، والابحاث، التي تخدم تحديد أطياف مستخدمي تقنيات المعلومات والاتصالات، من خلال فئاتهم العمرية، جنسهم، مكان تواجدهم، بما يسمح باستهدافهم، إعلانيا، وإعلاميا. وأحيانا كثيرة، تلجأ التطبيقات، إلى جمع بيانات حساسة، من خلال ما يسمى معلومات اختيارية، يترك للمستخدم ان يوافق على اعطائها، مثل: الميول الجنسية، والعرق، والحالة الاجتماعية الخ...

فالتطبيقات المجانية، على الهواتف الخليوية، والهواتف الذكية، كما محركات البحث، ومواقع التواصل الاجتماعي، والترفيه، وتنزيل الموسيقى، والتجارة الإلكترونية، وتطبيقات تحديد الاماكن، والخرائط الرقمية، طرق سريعة، ليس فقط للاتصال والوصول إلى المعلومات، بل أيضا لجمع البيانات، ورصد وتحركات الأفراد وعلاقاتهم من خلال نشاطهم في الفضاء السيبراني. فالآلة التي تعرف مستخدم الانترنت، أكثر ما يعرف نفسه، تسمح للبرامج التي يستخدمها، في الاستثمار مباشرة في خصوصيته، بما يساهم في نمو وازدهار الاقتصاد الرقمي[231].

وهكذا، يتعرض الحق في الخصوصية للانتهاك، نتيجة الدفق الهائل للبيانات الشخصية، عبر الفضاء السيبراني، ليس فقط من قبل السلطات الحكومية، الاجنبية منها والوطنية، وانما أيضا، من قبل المؤسسات التجارية، والمجرمين السيبرانيين، على حد سواء. ولذا، تعتبر حماية البيانات الشخصية، والحق في الخصوصية، من التحديات الأساسية، التي يواجهها مجتمع المعلومات، في سعيه إلى تعزيز الثقة، في الفضاء السيبراني.

٣. الحق في الخصوصية

بالرغم من الاعتراف به، من قبل العديد من الدول والشرع والقوانين[232]، يبقى الحق في الخصوصية، وتبقى حماية البيانات الشخصية، عرضة للاعتداء، ليس فقط نتيجة النقص التشريعي والتنظيمي، والممارسات الحكومية ، وانما نتيجة للامكانات التقنية الهائلة، التي تتيحها تقنيات المعلومات والاتصالات، والتي لا يمكن توقع امكاناتها. ونذكر هنا على سبيل المثال: تقنيات الرصد، وجمع البيانات، والتتبع، والمعالجة، والتنقيب، والوصول بسرعة فائقة، إلى عدد أكبر من الناس، في أماكن

[230] *Rapport « Collin et Colin ». Dans toute application en ligne, l'utilisateur est actif et son activité, peut être captée sous la forme de données. Les données sont un flux essentiel qui irrigue l'ensemble de l'économie numérique. - http://www.economie.gouv.fr/files/rapport-fiscalite-du-numerique_2013.pdf*

[231] *Personal data: Emergence of a new Asset class. http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf*

[232] – الحق في الخصوصية من الحقوق الاساسية، المعترف بها في عدد من البلاد حول العالم، وفي نصوص عالمية، مثل الدساتير الوطنية والاتفاقية. الإعلان العالمي لحقوق الانسان، شرعة الحقوق السياسية والمدنية، الاتفاقية الأوروبية لحماية حقوق الانسان والحريات، والاتفاقية الأميركية لحقوق الانسان.
- The Universal Declaration of Human Rights,(Article 17) of the International Covenant on Civil and Political Rights, (Article 8) of the European Convention on Human Rights, (Article 11) of the American Convention on Human Rights.
- Article 12 of the Universal Declaration of Human Rights states, "No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks."

مختلفة من العالم. يضاف إلى ذلك، استحالة معالجة النتائج السلبية للاعتداءات، في أحيان كثيرة، مع تعذر استعادة البيانات التي تم الاستيلاء عليها، أو تعذر السحب أو الالغاء الكامل للبيانات أو الاخبار، التي تم نشرها، أو تشويهها، أو تزويرها والتلاعب بها. ولا ننسى أيضا، الخطر الذي يمثله، اقتحام بعض قواعد المعلومات الشخصية، سواء منها تلك التي تحتفظ بها الشركات، أو تلك التي تحتفظ بها الجهات الرسمية[233].

ويعتبر هذا الحق من الحقوق الشخصية، المحمية في إطار الحريات العامة. فالخصوصية تعني، بشكل أساسي، المحافظة على سرية، أو على الأقل، على محدودية انتشار المعلومات، التي تسمح بتحديد الشخص، ونشاطه، ومكان تواجده، وعلاقاته الشخصية، الامر الذي يمنع التدخل، فيما يعتبره أمورا حميمة، أو حتى أسرارا، يمكنها ان تعرض استقراره، وسلامته المادية والمعنوية.

وعليه، هنالك اعتداء على الخصوصية، سواء تعلق الامر، بكشف سر دفين، ونشره إلى الآخرين، أم بمراقبة ورصد تحركات، لم يقترنا بكشف أسرار، أو بنشر معلومات حساسة. فالضرر واقع في الحالتين: اذ ينتج عن كشف المعلومات، في الحالة الأولى، وعن كون الشخص، وضع تحت المراقبة، في الحالة الثانية.

ويرتبط الحق في الخصوصية، بالحق في الحفاظ على الصورة، وبالحق في الحفاظ على السمعة. الا ان هذا الحق، وبالرغم من الاعتراف به، من قبل العديد من الدول والشرع والقوانين[234]، كالدساتير الوطنية، وشرعة حقوق الإنسان، وشرعة الحقوق المدنية والسياسية، والاتفاقية الأوروبية لحماية حقوق الإنسان والحريات، يتعرض للاعتداء، ليس فقط من قبل الجهات الرسمية في بعض البلدان، وانما أيضا، من قبل مستخدمي الانترنت أنفسهم. فمما لا شك فيه، ان الإمكانات الهائلة التي تتيحها الانترنت، لناحية الوصول إلى عدد أكبر من الناس، وبسرعة فائقة، في أماكن مختلفة من العالم، تجعل المخاطر التي يتعرض لها هذا الحق، أكبر وأدهى. والمثال الذي يمكن ايراده هنا، هو رصد حركة الأشخاص وملاحقتهم، كما التنصت على اتصالاتهم، والاطلاع على مراسلاتهم، إضافة إلى امكانية نشر صور شخصية وأخبار خاصة، أو تشويهها، أو تزويرها والتلاعب بها. يضاف إلى ذلك، الخطر الذي يمثله، اقتحام بعض قواعد المعلومات الشخصية، سواء منها تلك التي تحتفظ بها الشركات، أو تلك التي تحتفظ بها الجهات الرسمية[235]، بما يعنيه من خطر انكشاف، وتسرب معلومات.

وتزيد طبيعة النشاط في الفضاء السيبراني، تعقيدات الحفاظ على الخصوصية، كما عرفناها في العالم المادي. فكل حركة على جهاز الكومبيوتر، أو الهاتف النقال، أو أي جهاز متصل بالانترنت، تشكل معلومة يمكن جمعها، وتناقلها، ومعالجتها، وتحليلها. وهذا لا يحدث بدون موافقتنا القانونية على ذلك، عبر الضغط على زر "موافق" في سياسة الاستخدام، التي تخرج الينا، قبل البدء باستخدام اي تطبيق، أو برنامج. وغني عن القول، ان هذه العقود التي نوقع على قبولها، ليست في الحقيقة، الإقرارا

[233] منى الأشقر جبور ومحمود جبور- القانون والانترنت: تحدي التكيف والضبط- المنشورات الحقوقية- صادر- بيروت- ٢٠٠٨

[234] *The Universal Declaration of Human Rights, (Article 17) of the International Covenant on Civil and Political Rights, (Article 8) of the European Convention on Human Rights, (Article 11) of the American Convention on Human Rights.*

Article *12 of the Universal Declaration of Human Rights states, «No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks.»*

[235] منى الأشقر جبور ومحمود جبور- القانون والانترنت: تحدي التكيف والضبط- المنشورات الحقوقية- صادر- بيروت- ٢٠٠٨

بتنازلنا، عن حقنا في الخصوصية، عبر منح الشركة، مالكة التطبيق أو البرنامج حق التصرف في بياناتنا الشخصية. ويضاف إلى ذلك، خطر قبولنا، بالملاحقة أمام محاكم اجنبية، لا نملك القدرة الكافية على متابعة أنظمتها والقوانين، التي تطبق لديها. وفي حال امتلاكنا لهذه القدرة، تبقى التكلفة عالية، ومن الصعب تحملها.

ويترافق كل ذلك، مع ازدياد وتصاعد أعداد الكعكات cookies، التي تزرعها محركات البحث، والمواقع التي نزورها، بهدف متابعة نوعية نشاطنا، واهتمامتنا، وحركة تصفحنا للانترنت، وبما يساعد على تحديد أطيافنا، لاستهدافنا بإعلانات وأخبار، وخدمات تطابق شخصيتنا، واحتياجاتنا، وميولنا. ويحدث كل ذلك، دون ان ننتبه اليه، ودون ان ندرك كمية المعلومات، والبيانات الشخصية التي تجمع، والحد الذي وصل اليه، اختراق خصوصيتنا. ولا بد من الإشارة هنا، إلى بروز بوادر تشريعية، تنظم وتمنع عملية التتبع والرصد[236]، والتي تهدف قبل كل شيء، إلى حماية المستهلك، بما يعزز الثقة في البيئة السيبرانية.

ويعود الاهتمام بالمحافظة على الحق في الخصوصية، إلى بدايات استخدام تكنولوجيا المعلومات والاتصالات، وإنشاء قواعد البيانات الشخصية[237]. إلا أن اهتمام الدول، بالحفاظ على هذه الحقوق والحريات، يختلف باختلاف ثقافتها القانونية. ففي فرنسا، حيث القواعد الصارمة لحماية الحريات الشخصية، تتولى هيئة خاصة الرقابة على أمن المعلومات الشخصية، بينما لا توجد في الولايات المتحدة الأميركية، سلطة مشابهة لها[238]. وغني عن القول، ان الاختلاف بين الأنظمة القانونية، والمبادئ التي يتم على أساسها التعامل مع البيانات، يؤثر سلبا على الحماية القانونية للحق. ففي الولايات المتحدة الأميركية، تعتبر هذه البيانات، بيانات تجارية، ذات قيمة خاضعة لحاجات السوق، بينما تعتبر هذه البيانات في أوروبا، كجزء من خصائص الميزات الشخصية[239]، ما يجعل تعامل القضاء مع شروط استثمارها، ومعالجتها، يختلف بشكل أكيد.

وتتمثل الجوانب القانونية للاعتداء على الخصوصية، في عدد من الجرائم، والأعمال غير الشرعية، التي يمارسها الأفراد، أو الجهات الحكومية، ومنها: انتحال هوية الشخص، وانتحال الصفة، والابتزاز، واختراق أنظمة المعلومات، والوصول إلى الاسرار المهنية والتجارية، إضافة إلى الرصد غير المشروع لحركة الأشخاص والأموال، من قبل الأجهزة الحكومية، وتكوين ملفات معلومات، دون سبب شرعي، وكذلك التمييز العنصري، أو العقائدي، أو الديني.

[236] *The Do-Not-Track Online Act of 2013.*
[237] النص الأساسي حول الخصوصية وحماية المعلومات هو
“ *guidelines on Protection of Privacy and Transborder Flowa of Personal Data”.* في العام *1980. OECD. European Directive on Data Prtotection (95/46/EC)*
وفي نفس الاتجاه *The Council of Europe’s Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data. 1981.*
[238] *CNIL en France. Aux USA il ya Federal Trade Commission qui suit les dossiers internet et poursuit quelques sites web qui n’ont pas respecte sur leur site les déclarations sur la protection des données personnelles.*
[239] *L’oubli numérique, future droit constitutionnel? Selon Alex Türk, le président de la commission nationale de l’informatique et des libertés (CNIL) et président du G29 : « Pour les américains, les données personnelles sont des données commerciales qui ont une valeur marchande. En Europe, nous pensons que ce sont des attributs de la personnalité ». http://eulogos.blogactiv.eu/2009/11/23/1%2%80%99oubli-numerique-futur-droit-con*

أ- التوفيق بين مقتضيات الأمن والحفاظ على الحريات

- جمع البيانات واستخدامها

تجمع الحكومة البيانات الشخصية، بشكل متزايد، في إطار تأديتها لدورها في إدارة أمور المواطنين وشؤونهم الحياتية، ورغبة منها في حماية هؤلاء، وحماية سيادتها واستقرارها الأمني والاجتماعي والاقتصادي.

وتلجأ الحكومات المختلفة، إلى جمع البيانات الشخصية، التي تحدد هوية المواطنين، والمقيمين، مثل: بطاقات الهوية، والاستشفاء، والضمان الاجتماعي، وجوازات السفر، كما تلجأ السلطات إلى تعزيز مصداقية الهوية الشخصية، عبر إضافة البيانات البيومترية على العديد من الوثائق.

كذلك تستخدم البيانات الشخصية، وتنقل وتتبادل، تحت شعار الدفاع عن الأمن القومي، أو نتيجة التزام الدول، مكافحة بعض الأعمال والجرائم، ذات الارتدادات الكارثية: كالإرهاب مثلا. وفي هذا المجال، تستعمل البيانات الشخصية بشكل منهجي، من قبل الحكومات المختلفة، سواء في انشطتها الوطنية الداخلية، أو في علاقاتها مع الدول الاخرى، من خلال اتفاقيات[240]، أو من خلال أنظمة أمن، وبرامج متخصصة[241].

وعليه، تتشكل مصادر الخطر على الخصوصية، نتيجة الاستخدام غير القانوني للبيانات الشخصية، أي دون اعتبار لحقوق اصحابها، لاسيما حقهم في الخصوصية، وذلك، في القطاعين العام والخاص، على السواء.

لذا، لا بد من رسم حدود واضحة، لا يمكن للدولة ان تتجاوزها، منعا للاعتداء على الحريات والحقوق. والمثال الذي يمكن اثارته هنا، هو التشريعات[242] التي وضعت في العديد من الدول، بعد اعتداءات الحادي عشر من أيلول ٢٠٠١، تحت عنوان مكافحة الإرهاب. فقد اقرت في الولايات المتحدة الأميركية مثلا، صلاحيات واسعة للحكومة، واعطي هامش اوسع للتحقيق، واستبعدت المسؤولية عن أشخاص القانون الخاص، في حال افشائهم معلومات للحكومة. وكان البرلمان الأوروبي، قد اعرب عن قلقه، ازاء الأثر الذي يمكن لإجراءات تستهدف تحقيق الأمن، ان تتركه على الحقوق والحريات، وفي مقدمها الحق في الخصوصية[243].

بالمقابل، لا ينبغي حماية الأمن القومي، بمعزل عن الحقوق الأساسية والحريات المدنية للمواطن. فبين تحقيق الأمن القومي، وحماية الحقوق والحريات، لا بد من مراعاة التوازن، الذي يضمن عدم دفع هذه الأخيرة، إلى مستوى متدن، لتأمين مستوى عال من الأمن. وترتبط حماية البيانات الشخصية،

[240] *Les accords entre l'union européenne et les états unis.*
* *le traite de prum, signe le 27 Mai 2005*
[241] *Les systèmes d'échanges d'informations crées a l'échelle de l'Union Européenne : le système d'information Schengen (SIS), le système d'information douanier, et le système d'information d'Europol et celui d'Eurojust.*
[242] *Le Patriotact aux états unis. - plan d'action contre le terrorisme adopte par le parlement européen et modifie le 25 Mars 2004 suite aux attentats de Madrid puis suite aux attentats de Londres du 7 juillet 2005*
- recommandation relative a l'élaboration de « profiles terroristes » adoptée par le conseil européen en 2002
- directive du 15 Mars 2006 qui a prévu la conservation des données téléphoniques par les operateurs.
[243] *Résolution du 14 janvier 2009 sur la situation desdroits fondamentaux dans l'Union européenne (2004-2008). le Parlement européen « se préoccupe du fait que la coopération internationale dans la lutte contre le terrorisme a souvent abouti à unebaisse du niveau de protection des droits de l'Homme et des libertés fondamentales,notamment du droit fondamental au respect de la vie privée, à la protection des données à caractère personnel et à la non-discrimination*

ارتباطا وثيقا، بالأمن القومي للدولة. ويعود السبب في ذلك، إلى خطورة انكشاف معلومات خاصة، بالمواطنين عامة، وببعض اصحاب المراكز الحساسة، بشكل خاص، نظرا لامكانات الضغط التي يمكن ان تمارس عليهم نتيجة لذلك، بهدف ابتزازهم في عمليات إستخباراتية، تؤذي استقرار البلاد، وتعرض اقتصاده، أو نسيجه الاجتماعي، للانهيار.

يضاف إلى ذلك، اعتبار حماية البيانات الشخصية، عنصرا من عناصر تعزيز الثقة في الفضاء السيبراني، لاسيما فيما يخص تأمين المعاملات الإلكترونية، ومحاربة الجريمة السيبرانية.

ـ البيانات الشخصية للمسافرين

تستدعي مكافحة الجرائم العابرة للحدود، كتبييض الأموال، والإرهاب، والاتجار غير المشروع بالمخدرات، اهتماما خاصا وغير مسبوق، من قبل الحكومات المختلفة، بالبيانات التي تنتقل عبر الانترنت، ووسائل الاتصال الاخرى. فالبيانات الشخصية، تجمع بكميات كبيرة من المسافرين، ومن الوافدين إلى اي بلد، وتنظم في لوائح وقواعد معلومات، ويتم تبادلها، في محاولة لرصد التحركات المشبوهة. ويشكل هذا الموضوع، عقبة أساسية، أمام امكانية الحفاظ على الحق في الخصوصية، اذ انه يفقد صاحب البيانات، امكانية السيطرة عليها.

وتفرض القوانين الأميركية، في هذا المجال، على شركات الطيران، التي تقدم خدمات النقل، من والى أراضيها، أو عبر المرور بها، أن تزود وزارة الداخلية الأميركية[244]،بالبيانات الشخصية للركاب. ويهدف هذا الإجراء، إلى المساهمة في تأمين سلامة الطيران، بشكل عام، والحفاظ على أمن الولايات المتحدة، بشكل خاص. وتتوزع هذه البيانات على فئتين:

١. البيانات الخاصة باسم المسافر وسجله[245]، والتي تمثل المعلومات التي تقدم خلال عملية الحجز لدى الشركة، عن تفاصيل الرحلة، مثل: اسم المسافر، وتاريخ الرحلة، ونقطة الانطلاق والوصول، ورقم المقعد، وعدد الحقائب، إضافة إلى تفاصيل خاصة بالحجز، مثل: اسم وكالة السفر التي أجرت الحجز، وتفاصيل ايفاء قيمة التذكرة، وانضمامه إلى برامج خاصة بالزبائن، أو غيرها.

٢. البيانات الأكثر تحديدا[246]، وتتناول: المعلومات التي تؤخذ من جواز السفر، والتي تجمع خلال عملية التسجيل، والتي تقدم إلى السلطات المختصة بمراقبة الحدود، قبل الوصول، وذلك، للتأكد من أن المسافر، لا ينتمي إلى لائحة الأشخاص، الذين يمثلون خطرا على سلامة الطيران.

وكانت الولايات المتحدة الأميركية، قد وقعت في هذا الإطار، اتفاقا مع الاتحاد الأوروبي، في ١٦ تشرين الأول (اكتوبر) ٢٠٠٤، يفرض على هذا الأخير، أن يتأكد من التزام الناقلين الجويين، بتقديم هذه المعلومات[247]، كما هو مطلوب، إلى وزارة الداخلية الأميركية. ويتيح الاتفاق المذكور، امكانية الحصول على هذه المعلومات، بالطريقة الإلكترونية، وبشكل مسبق، لقيام الرحلات أو وصولها، ما يعني اتاحة امكانية توقع المخاطر، وتجنبها، بفاعلية أكبر.

[244] *US Department of Homeland Security.*
[245] *Passenger Name Record (PNR).*
[246] *(Advanced Passenger Information (API)).*
[247] *décision de la Commission 2004/535/EC:*
http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_235/l_23520040706en00110022.pdf

في المقابل، يمكن للاتحاد الأوروبي، وبحسب هذا الاتفاق، أن يطلب من الولايات المتحدة الأميركية، تزويده بيانات شخصية ، حول المسافرين من الولايات المتحدة الأميركية إلى أوروبا، في حال اعتماده لسياسة مشابهة، لتلك التي تعتمدها حاليا. ويأتي ذلك، في إطار المحادثات التي يقودها الاتحاد الأوروبي، في المنظمة العالمية للطيران المدني، من أجل تحديد معايير عالمية، حول استخدامات المعطيات الخاصة بالمسافرين، بهدف الحماية على المعابر، وفي النقل الجوي.

وقد جاءت الضمانات التي تلتزم بها الولايات المتحدة الأميركية، لتأمين مستوى حماية مقبول في الاتحاد الأوروبي، على الشكل التالي:

- حصر البيانات التي تنقل إلى الولايات المتحدة الأميركية، ضمن ٣٤ فئة، وهي أقل من تلك التي تجمع وتحفظ من قبل الولايات المتحدة الأميركية، عادة.
- حظر نقل البيانات التي تعتبر حساسة، والخاصة بالدين أو الصحة. وفي حال نقلها، يجري تنقيتها والغاؤها فيما بعد.
- حصر استعمال هذه البيانات ، بأهداف مكافحة الإرهاب، والجرائم الكبرى.
- محو هذه البيانات، بعد فترة زمنية، حددت بثلاث سنوات وثلاثة أشهر، ما عدا حالات مراجعتها، في إطار تحقيقات خاصة، أو مراجعتها يدويا.
- الزام الولايات المتحدة الأميركية، إعلام المسافرين، بهدف جمع هذه المعطيات ومعالجتها، وبهوية المسؤول عن المعالجة.
- إقرار حق أصحاب البيانات في النفاذ اليها، لمراجعتها وتصحيحها.
- إقرار صلاحية السلطات المختصة في الاتحاد الأوروبي، مساعدة الأفراد، لتقديم شكوى أمام السلطات الأميركية.
- منع فرز المعلومات، من قبل السلطات الأميركية، الا وفقا لكل حالة على حدة، ولأهداف متفق عليها.
- حظر نقل البيانات، إلى جهات أميركية، أو هيئات أخرى، وطنية أو أجنبية، الا بعد ابلاغ سلطة مختصة، يعينها الاتحاد الأوروبي.
- وضع تقرير سنوي، من قبل الهيئات المختصة، على المستوى الأوروبي، حول مدى احترام الولايات المتحدة الأميركية لالتزاماتها.

ويمكن للهيئات المكلفة حماية البيانات الشخصية، ممارسة صلاحيتها، في وقف انتقال البيانات إلى وزارة الداخلية الأميركية، بهدف حماية الأشخاص، من معالجة هذه البيانات، بطريقة مخالفة، لما جاء في الاتفاق مع الاتحاد الأوروبي.

في العام ٢٠١٢، وقع الاتحاد الأوروبي والولايات المتحدة الأميركية، اتفاقا آخرا، حول نقل بيانات المسافرين، يقضي بما يلي:

- مشاركة ملفات بيانات المسافرين، والتحليلات الخاصة بها، مع الهيئات القضائية في الاتحاد الأوروبي، لمكافحة الجرائم العابرة للحدود، والإرهاب، وتفعيل الملاحقات

- التزام الولايات المتحدة الأميركية، استخدام هذه البيانات في مكافحة الإرهاب، والجرائم الخطيرة، مثل تهريب المخدرات، والرقيق، والجرائم التي تصل عقوبتها الدنيا، إلى ثلاث سنوات حبس.
- تحديد مدة الاحتفاظ بهذه البيانات ب ١٠ سنوات، على ان يبقى الرجوع إليها ممكنا لمدة ١٥ سنة، لقضايا تتعلق بمكافحة الإرهاب، وعلى ان تتم معالجة البيانات، بطريقة تمنع التعرف على اصحابها، بعد مرور ٦ أشهر من تلقي السلطات الأميركية لها، ونقلها إلى قاعدة معلومات غير موضوعة في الخدمة، بعد مرور ٥ سنوات، وحيث لا يمكن للمسؤولين الأميركيين الوصول اليها، الا ضمن شروط معينة.
- تعيين مسؤول عن حماية البيانات الشخصية، في وزارة الداخلية الأميركية، يقدم تقارير حول الموضوع إلى الكونغرس، ويتابع قضايا الحماية مع الهيئات المسؤولة، في الاتحاد الأوروبي، كما يتابع الشكاوى، التي تقدم بها مواطنون، اعتبروا ان الولايات المتحدة، لا تلتزم احترام خصوصيتهم.
- اتاحة الامكانية أمام المواطنين الأوروبيين، للاعتراض على حفظ البيانات، وتقديم الشكاوى الادارية والقضائية، وتصحيح البيانات، والمطالبة بمحوها.
- التزام الناقل، إعلام المسافرين، بأهداف وكيفية استخدام بياناتهم، وآليات ممارسة حقوقهم.
- منع تحديد اطياف المسافرين، على أساس معالجة آلية، ومنع الملاحقة على هذا الأساس.
- استخدام محدد للبيانات الحساسة، مع التزام تطبيقات تمنع معالجة البيانات الحساسة.
- وضع آليات ادارية، واصول تقنية، تضمن أمن البيانات، ضد التلف والمحو والتلاعب، وغير ذلك من أخطار. ويفترض في هذا المجال، تشفير البيانات.

ب– تآكل الحق في الخصوصية

ـ الرقابة ومتطلبات الثقة

بعد ان تحولت الانترنت، إلى مساحة مفتوحة لتبادل المعلومات، والوصول إلى الخدمات، وتوسيع أفق الفرد الفكرية، والاجتماعية، والاقتصادية، والمعرفية، رأت الدول المختلفة، بوادر تهديدات مباشرة لامنها القومي، وبدأت بالاعتماد على تقنيات المعلومات والاتصالات، وعلى الانترنت وكل ما يتصل بها من اجهزة، لممارسة رقابتها، سواء بطريقة شرعية تنسجم مع دورها في حفظ الأمن، أو بطريقة غير شرعية تعارض الشرع الدولية لحقوق الإنسان وحرياته، كما لمختلف الإعلانات التي اقرت، حرية الانترنت، وحرية تبادل المعلومات، والحق في الوصول إلى المعرفة. فعمد العديد من الحكومات، إلى سياسات قمعية تبلورت في سياسات حجب المواقع، وجمع البيانات ذات الطابع الشخصي، والتنقيب في البيانات للتحري عن الأشخاص والاسرار، وملاحقة المدونين، أو مستخدمي الشبكات الاجتماعية، دون اعتبار لحقوق الإنسان. وفي هذه الممارسات غير الشرعية، جينات مشابهة لتلك الموجودة، في الجريمة، والاعتداءات السيبرانية، كونها تزعزع الثقة في الفضاء السيبراني، وتمنع حركة التدفق الحر للمعلومات، وتعيق ممارسة الحريات والحقوق.

وغني عن القول، ما لهذا من تأثير سلبي، حيث تؤدي هذه الممارسات، إلى عزل الفرد عن عالم المعرفة، وتؤثر في تكوينه الفكري، عندما تقدم له صورة مغلوطة أو غير مكتملة عن العالم، عدا عن انها تساهم في منع تقدم المجتمع ككل.

مما لا شك فيه، انه لا اعتراض على حق الدولة في ممارسة الرقابة على المحتوى، في الفضاء السيبراني، انطلاقا من واجبها، في حفظ الأمن والنظام العام، كأن تلاحق الجريمة السيبرانية، والاعتداءات على حقوق الملكية الفكرية، والحض على مخالفة القانون، وكل عمل من شأنه الاساءة إلى المجتمع، وإلى سيادة الدولة. الا ان دورها هذا، لا يجوز ان يتحول إلى دور قمعي، يمنع حرية التعبير، وحرية تبادل المعلومات، لانه يتعارض بشكل أساسي، مع مبادئ ومتطلبات الثقة والأمن في الفضاء السيبراني، والتي تقوم على:

- حرية دفق المعلومات، دون اي حد منها، الا لأسباب قانونية، وبحسب ما تقره القوانين الدولية، والتشريعات.
- احترام القواعد القانونية الخاصة باصول التحقيق، والتجريم، والملاحقة، بما ينسجم مع احترام القوانين الخاصة بحقوق الإنسان وحرياته.
- دعم الجهود الدولية في مكافحة الجريمة السيبرانية.
- الحرص على منع الاعتداء على المستخدمين، واستغلالهم، والتعدي عليهم.
- احترام الخصوصية والحريات، في كل التطبيقات الخاصة بأمن الشبكات والاتصالات.

لكن الواقع، وبرغم المبادئ والإعلانات، يبقى مغايرا، وشديد الخطورة، حيث تتكاثر وتتكثف الرقابة، كما ونوعا، لتصبح شاملة. فمع تطور امكانات تقنيات المعلومات والاتصالات، وتنوعها، وتوسع الاتكال عليها، في تدبير شؤون الحياة اليومية، وانتشار شبكات التواصل الاجتماعي، تزداد امكانات الرصد، والتتبع، والتنصت، وتجميع المعلومات، ومعالجتها.

- الرقابة الشاملة

تحتل أخبار انتهاك الحق في الخصوصية والحريات المدنية، وحرية التعبير على الانترنت، الصفحات الأولى، في وسائل الإعلام. فمن ويكيليكس[248]، إلى تامبورا[249] في بريطانيا، إلى سنودين[250] وبريسم[251]في الولايات المتحدة الأميركية، إلى برامج الاستخبارات في كندا[252]، إلى تشديد الرقابة على الانترنت في

[248] *https://wikileaks.org/*
[249] *Tempora, is a clandestine security electronic surveillance program tested in 2008,[2] established in 2011 and operated by the British Government Communications Headquarters (GCHQ). Tempora uses intercepts on the fibre-optic cables that make up the backbone of the internet to gain access to large amounts of internet users' personal data. http://en.wikipedia.org/wiki/Tempora*
[250] *http://edition.cnn.com/2013/09/11/us/edward-snowden-fast-facts/*
En *juin 2013, l'informaticien de la National Security Agency (NSA) américaine, Edward Snowden, révélait l'existence de programmes de surveillance. Le plus connu, nommé PRISM, permet au gouvernement américain d'accéder directement aux serveurs de neuf compagnies: Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple. La NSA aurait ainsi, en mars 2013, récupéré 97 milliards d'informations. http://www.la-croix.com/Actualite/Monde/Pourquoi-il-faut-reformer-Internet-2014-04-23-1140281*
[251] *Special source operation system legally immunized private companies that cooperate voluntarily with U.S. intelligence collection.*
[252] *Attention fliers: Canada's electronic spy agency is following you - new Snowden leaks.http://rt.com/news/canada-snowden-spying-nsa-airport-442/*

فنزويلا[253]، وسورم ٢ وسورم ٣ والسجل الواحد في روسيا[254]، واتخاذ إجراءات تضمن تحديد هوية الأشخاص[255]، وحجب مواقع التواصل الاجتماعي، والجدار العظيم في الصين[256]، تأكيد على اهمية البيانات الشخصية، وضرورة حمايتها، لمنع استغلالها في الاساءة إلى حقوق الأفراد، وفي الوصول إلى مستخدمي وسائل الاتصالات، دون وجه حق.

وكانت تصريحات سنودين، وكشف عمليات تجسس الولايات المتحدة الأميركية، على الدبلوماسيين، والسياسيين، والمواطنين، كما الاجانب، قد أثارت موجة من الاستياء حول العا لم، أدت فيما أدت ، إلى قيام الرئيسة البرازيلية بالدعوة لعقد قمة دولية حول مستقبل الانترنت، تناقش فيها، بشكل أساسي، حقوق الدول المختلفة في سياسة إدارة الانترنت، وحماية الحقوق، لاسيما الحق في الخصوصية، وحماية البيانات الشخصية[257].

فمع دفق المعلومات، وتصاعد استخدام الهواتف الخليوية، وتضخم امكانات الاتصال، يتحول كل فرد منا، إلى لاقط عند أجهزة الاستخبارات الدولية[258]، اذ تتطور سبل الرقابة، ووسائل جمع المعلومات، وأساليب رصدها، ومعالجتها، واستثمارها، وتحليلها، والتنقيب عنها.

وبالفعل، يعتبر الفضاء السيبراني، مرآة للفضاء المادي، الذي تعودنا ان نتحرك خلاله. لذا، كان من الطبيعي، ان تحاول الأجهزة الحكومية المختلفة، التعامل مع البيانات الشخصية والمعلومات، من منطلق ضرورة الرقابة والسيطرة. وقد تطورت هذه المحاولات، بشكل دراماتيكي، وازدادت حدة الرقابة على البيانات والاتصالات الشخصية، بعد احداث الحادي عشر من أيلول في الولايات المتحدة الأميركية، حيث ارتبطت هذه الرقابة، بحجة مكافحة الإرهاب، والحرب عليه. وتستخدم العديد من الدول، برامج رقابة متطورة، كما أسلفنا، كما تلجأ معظم شركات الاتصال الكبرى، إلى تسليم البيانات والمعلومات، إلى ادارات وطنية أمنية.

وتستفيد هذه الأخيرة، من مقارنة البيانات التي تسلم اليها، بما جمعته من بيانات ولوائح، ومن تعقب الأفراد عبر تطبيقات تحديد المواقع، والوصول إلى لوائح اصدقائهم، وأفراد عائلتهم، وبيانات اتصالاتهم على الهاتف الذكي، والبيانات الجغرافية الموجودة، على الصور التي يتبادلونها على مواقع التواصل الاجتماعي، عبر هواتفهم، وبريدهم الإلكتروني. وكانت اجهزة الاستخبارات البريطانية، قد اشارت في مستندات سرية، إلى ان القدرة على التجسس، موجودة في برامج الالعاب الأكثر انتشارا، لاسيما عندما تسمح بتحديد موقع الشخص، وعمره، ومكانه، وجنسه، وغير ذلك من بياناته الشخصية[259].

[253] *Venezuelan Government Expands Internet Censorship- http://mashable.com/2014/02/20/venezuela-social-media/*
[254] *In Ex-Soviet States, Russian Spy Tech Still Watches You-By Andrei Soldatov and Irina Borogan- 12.21.12- 6:30 AM. http://www.wired.com/dangerroom/2012/12/russias-hand/all/*
[255] *China orders real name register for online video uploads. http://www.reuters.com/article/2014/01/21/us-china-internet-idUSBREA0K04T20140121*
[256] *King, Gary, Jennifer Pan, and Margaret Roberts. 2014. Reverse Engineering Chinese Censorship through Randomized Experimentation and Participant Observation. Copy at http://j.mp/16Nvzgehttp://gking.harvard.edu/publications/randomized-experimental-study-censorship-china*
[257] *-Pourquoi il faut réformer Internet.*
http://www.la-croix.com/Actualite/Monde/Pourquoi-il-faut-reformer-Internet-2014-04-23-1140281
[258] *We are "somehow becoming a sensor for the world intelligence community" - Philippe Langlois- founder of the Paris-based company Priority One Security, on agencies' ability to harvest personal data from users of smartphones. http://www.nytimes.com/2014/01/28/pageoneplus/quotation-of-the-day-for-tuesday-january-28-2014.html?_r=0*
[259] *Lisa Vaas on January 29, 2014- Spy agencies are slurping personal data from leaky mobile apps- http://nakedsecurity.sophos.com/2014/01/29/spy-agencies-are-slurping-personal-data-from-leaky-mobile-apps/- consulted on 30/1/2014*
- A secret British intelligence document, from 2012, said that spies can scrub smart phone apps to collect details, like a user's "political alignment", and sexual orientation.

وغني عن القول، ما يمثله هذا الواقع، من تهديد جدي للحياة الخاصة، ومن خلالها للحريات المدنية والحقوق الشخصية الاخرى، التي تعتبر أساسية في ارساء قواعد الديمقراطية، والحكومة الرشيدة [260]. ففي الأنظمة الديمقراطية، ومنها النظام اللبناني، ان حكم القانون، وحرية التعبير، والمجتمع المدني، تعزز حماية الحريات، في مواجهة ممارسات الأنظمة الاستبدادية: اساءة استخدام السلطة، والتعسف في استخدام الحق، وغياب المحاسبة، والاعتقال غير القانوني.

وعليه، ان الرقابة الشاملة Mass Surveillance، والتحكم بوسائل الاتصالات المختلفة، وجمع البيانات عنها، لتعقب الأفراد والمؤسسات، تهدد الحريات، بدء من حرية المعتقد، والرأي والتعبير، وصولا إلى حرية ممارسة النشاط السياسي والاجتماعي، بما يهدد الثقة ويؤثر الاقتصاد ونموه[261]، ويقوض اسس النظام الديمقراطي[262].

وقد رأى القضاء الأميركي، ان هذه الرقابة الشاملة، تشكل تعديا صريحا على الحريات. ففي قضية مرفوعة من الاتحاد الأميركي للحريات المدنية، ضد عدد من الأجهزة الأمنية والاستخباراتية، ووزير الدفاع، على خلفية التنصت على المواطنين الأميركيين، وجمع بيانات اتصالاتهم وبياناتهم الشخصية، اعتبرت محكمة في نيويورك، ان هذا العمل، يخرج عن الصلاحيات المعطاة لهذه الهيئات، في إطار مهمتها لحفظ الأمن القومي، ويخالف التعديلين الأول والثاني من الدستور، اللذين يقران حرية التعبير، وحق الشخص في عدم انتهاك حرمة مسكنه، دون وجه حق[263].

- تحالف الخمس عيون

على أثر الحرب العالمية الثانية، وفي رد على تحديات تثبيت الأمن، عمد عدد من الدول، إلى إنشاء تحالف استخباراتي، عرف ب "تحالف الخمس عيون"، وأعلن عنه، كشرعة "عدم تجسس"[264] بين الدول المتعاقدة. ويتألف هذا التحالف، من الوكالة الوطنية للأمن في الولايات المتحدة الأميركية، وقيادة الاتصالات في المملكة المتحدة، ووزارة الاتصالات في كندا، ومكتب أمن الاتصالات في في نيوزيلندا، ومديرية الاشارات في استراليا. وهو عبارة عن تحالف استخباراتي، يغطي برامج تجسس، وتبادل معلومات، ذات أبعاد عالمية، حيث يطاول معظم أنظمة الاتصالات في العالم. بدأ هذا التحالف

[260] *"The right to privacy, the right to access to information and freedom of expression are closely linked. The public has the democratic right to take part in the public affairs and this right cannot be effectively exercised by solely relying on authorized information." Ms. Pillay- UN High Commissioner for Human Rightshttp://www.un.org/apps/news/story.asp?NewsID=46780&Cr=privacy&Cr1=#.UwCw6ThWHZY*

[261] *The NSA overreach poses a serious threat to our economy. http://www.theguardian.com/commentisfree/2013/nov/20/jim-sensenbrenner-nsa-overreach-hurts-business*

[262] *UNGA- 16 May 2011 A/HRC/17/27- Human Rights Council- Seventeenth session- Agenda item 3 - Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development "The growing use and sophistication of digital surveillance has outstripped the ability of societies to legislate their proper use, leading to "ad hoc practices that are beyond the supervision of any independent authority," and that threaten to repress free expression"*

[263] *United states district court southern district of New York. 13 Civ. 3994- June 11 2013- https://www.aclu.org/files/assets/nsa_phone_spying_complaint.pdf*

[264] *No Spy Act*

عمله في العام ١٩٤٦، ووضع عددا من اتفاقات التعاون، عرفت ب "UKUSA"[265]، نسبة إلى أسماء الدول التي اقرته.

وقد أبرزت تصريحات سنودين، في العام ٢٠١٣، العلاقة الوثيقة بين أعضاء هذا التحالف، حيث وضعت رموز خاصة به، على معظم الوثائق السرية، التي يمكن تبادلها بين هذه الدول. ويتميز التعاون بدرجة عالية من التنسيق، بين اعضائه، يصعب معها، تمييز البلد، مصدر الوثيقة. ولعل المثال الاوضح، على عمق هذا التنسيق، هو برنامج التنصت والرصد، Tempora[266]، الذي كشف سنودين عن وجوده[267]. ويعمل هذا البرنامج، منذ العام ٢٠١١، على عزل معظم الاتصالات، التي تجمع عبر عصب الانترنت، اي الكابلات البصرية، لمعالجتها فيما بعد[268].

أما مراكز التنصت، فموجودة اما في المملكة المتحدة، واما خارجها، بمعرفة من الشركات مالكة الكابلات. وتعمل أجهزة الاستخبارات الأميركية والبريطانية معا، على تحليل البيانات المجموعة، من الاتصالات الهاتفية، والأجهزة الذكية، ومواقع الانترنت. وقد وضع كل من الأجهزة، عددا من الكلمات المفاتيح، التي يتم البحث من خلالها. وترتكز عملية التنقيب عن البيانات، في ما يعزل من اتصالات، على برنامج أساسي هو XKEYSCORE[269]، وهو إطار تحليلي، يسمح بتفتيش كم هائل من بيانات جمعت على مدى ثلاثة ايام، في مئة وخمسين موقعا عالميا، على سبعمائة قاعدة معلومات، وذلك، من خلال عملية واحدة.

ويوثق هذا البرنامج، إضافة إلى عناوين البريد الإلكتروني، أسماء الملفات، وعناوين الانترنت، والكعكات، والأسماء في لوائح الاصدقاء، وارقام الهواتف، والبيانات الوصفية Metadata، التي تسجل من عمليات تصفح الانترنت، وتطبيقات الهواتف الذكية. يؤمن أمن هذا البرنامج، أسهل الطرق وأسرعها، إلى جمع بيانات ومعلومات خاصة، حول اي كان في العالم، من خلال عنوان بريد إلكتروني. وإذا تخيلنا لائحة العناوين، في بريد كل شخص، لا مكننا تصور سيناريو اختراق ايميل واحد والحصول عليها، لنعرف حجم الانفلاش العشوائي للرقابة، التي تمارسها هذه الأجهزة. وكان يكفي، بحسب تصريحات سنودين، ان يكون لديه، عنوان بريدي، حتى يدخل من خلاله إلى بيانات صاحبه،

[265] *https://en.wikipedia.org/wiki/UKUSA_Agreement - The United Kingdom – United States of America Agreement (UKUSA, /jukus/ ew-koo-sah)[1][2] is a multilateral agreement for cooperation in signals intelligence between Australia,Canada, New Zealand, the United Kingdom and the United States. The alliance of intelligence operations is also known as the Five Eyes. [In classification markings this is abbreviated as FVEY, with the individual countries being abbreviated as AUS, CAN, NZL, GBR and USA respectively.*
Emerging from an informal agreement related to the 1941 Atlantic Charter, the secret treaty was renewed with the passage of the 1943 BRUSA Agreement, before being officially enacted on 5 March 1946 by the United Kingdom and the United States. In the following years, it was extended to encompass Canada, Australia and New Zealand. Other countries, known as «third parties», such as West Germany, the Philippines and several Nordic countries also joined the UKUSA community.
[266] *Tempora is the codeword for a formerly secret computer system that is used by the British Government Communications Headquarters(GCHQ).*
[267] *GCHQ taps fibre-optic cables for secret access to world›s communications- «The existence of the programme has been disclosed in documents shown to the Guardian by the NSA whistle blower Edward Snowden as part of his attempt to expose what he has called «the largest programme of suspicionless surveillance in human history».*
https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
[268] *GCHQ taps fibre-optic cables for secret access to world›s communications- Exclusive: British spy agency collects and stores vast quantities of global email messages, Facebook posts, internet histories and calls, and shares them with NSA, latest documents from Edward Snowden reveal. https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa*
[269] *XKeyscore: NSA tool collects ‹nearly everything a user does on the internet›. A top secret National Security Agency program allows analysts to search with no prior authorization through vast databases containing emails, online chats and the browsing histories of millions of individuals, according to documents provided by whistleblower Edward Snowden. The NSA boasts in training materials that the program, called XKeyscore, is its "widest-reaching" system for developing intelligence from the internet. https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data*

خلال دقائق، وربما ثوان[270].

هذا، وتقوم كل وكالة في دولة من دول التحالف، بجمع وتحليل جميع البيانات، التي تمر في اراضيها، إضافة إلى تلك، التي لا تمر فيها.

وقد أظهرت الوثائق، كما المعلومات المسربة، كيف تسلل هذا التحالف، إلى معظم اشكال الاتصالات الحديثة، عبر ممارسات تمثلت، في اجبار الشركات التي تعمل في مجال تقنيات المعلومات والاتصالات، على تسليم بيانات زبائنها، وفي تسجيل بيانات الاتصالات، بين مراكز المعلومات العائدة إلى هذه الشركات، والوصول إلى بيانات حساسة يتم تبادلها على SWIFT[271]، وهو شبكة تتبادل عليها المصارف، وبقية المؤسسات المالية، المعلومات المالية، بطريقة موثوقة، في بيئة موحدة المقاييس والمعايير.

وتعتبر هذه الممارسات، تهديدا مباشرا لأمن الشبكة العالمية للاتصالات، كونها تضعف الثقة في الفضاء السيبراني، وفي نظام تبادل المعلومات، كما في مصداقية برامج وشركات الترميز. ويعتمد هذا التسلل، بشكل أساسي، على اختراق مجال عملت هذه الدول نفسها على تحصينه، بعدد من القواعد والمقاييس التقنية، التي تضمن ترميزه بشكل موثوق.

ـ ممارسات غير مقوننة

مع التقنيات، تغير العالم، ولم تعد البيانات تجمع في ملفات ورقية، وادراج وخزائن مقفلة، بل في مراكز غير معروفة، ومنتشرة حول العالم. وأصبحت الاتصالات من الممارسات اليومية لكل فرد وإدارة، كما خرجت تفاصيل الحياة اليومية إلى العلن، عبر مواقع التواصل الاجتماعي، كذلك انتشر التعبير عن الرأي، وتبادل الافكار.

في المقابل، تتصف مسارات الاتصالات، واماكن وجود المخدمات، التي تحفظ البيانات، كما الجهة التي تنتقل اليها، بالمجهولية. فما من مستخدم يمكنه الإحاطة بمسار البيانات التي يرسلها عبر الانترنت، أو عبر هاتفه. ولكن الأكيد، اننا جميعا ندرك، ان البنية التحتية العالمية للانترنت والاتصالات، تمر عبر بلدان عديدة، وان الحوسبة السحابية، تؤمن إيواء البيانات، في بلدان صديقة، أو عدوة، أو محايدة، ما يعرضها للاختراق، وللتنصت من قبل عدد من أجهزة الاستخبارات.

اما ما يشكل الخطر الأكيد، فهو ان دول التحالف، لم تضع إطارا تشريعيا، ينظم شروط وحالات عمليات التنصت، وجمع، وتبادل المعلومات، سواء عن المواطنين أو عن المقيمين، التي تقوم بها إحدى وكالات الاستخبارات، العضو في التحالف، على ارض دولة اخرى من دوله، كما لا يوجد إطار تشريعي، يحدد حالات شرعية طلب معلومات الاتصالات والانترنت، والبريد الإلكتروني، من الشركات الخاصة.

ومما لا شك فيه، ان هذه الممارسات، تسقط الحق في الخصوصية، الذي التزمت به، من خلال التزامها الإعلان العالمي لحقوق الإنسان، والذي ينص على عدم جواز التدخل الاعتباطي وغير الشرعي، في

[270] *Indeed, training documents for XKEYSCORE repeatedly highlight how user-friendly the program is: with just a few clicks, any analyst with access to it can conduct sweeping searches simply by entering a person's email address, telephone number, name or other identifying data. There is no indication in the documents reviewed that prior approval is needed for specific searches. https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/*
[271] *Society for Worldwide Interbank Financial Telecommunication (SWIFT)*

خصوصية الفرد، أو شؤونه العائلية، أو مراسلاته، كما لا يجوز الاعتداء على سمعته. فبمقتضى هذه الشرعة، يبقى الحق في الخصوصية قائما، ومعترفا به، بغض النظر عن الدول، والسيادات المختلفة، التي تمر بها بيانات الاتصالات.

على خط موازٍ، تعتبر الرقابة الشاملة، التي كشفها سنودين، مخالفة للقانون الدولي، الذي يقر حقوق الإنسان، لاعتبارات عديدة، ليس أقلها انها تحدث، دون اي تمييز، بين شخص مشبوه، وآخر لا غبار على سلوكه، ودون مسوغ شرعي، ودون اذن من السلطات المختصة، لمعظم الاتصالات، وعمليات تبادل المعلومات، ودون ادراك من الأفراد الذين تطالهم الرقابة، لاي من اصولها وأبعاده، بما يعني انها تطال أفرادا لا علاقة لهم باي من النشاطات، التي يسعى الأمن إلى ضبطها، وبانها تبقى بعيدة عن حق المواطن أو المقيم، في الاعتراض على انتهاك حقوقه، التي تقرها القوانين والشرع الدولية.

وفي هذا، ما فيه من مخالفة لمبدأ "تطبيق القاعدة القانونية"، في مجتمع ديمقراطي، ولمبدأي الشفافية والمحاسبة. يضاف إلى ذلك، التأثير غير المباشر على حرية التعبير، نتيجة خوف مستخدمي الانترنت من الرقابة، ما ينتقص من اهمية الانترنت، كوسيلة تعبير ديمقراطي، وتواصل، وانفتاح، وتطور. هذا، عدا عن الخطر الذي تشكله هذه الرقابة، على الحق في الخصوصية.

٤. الشبكات الاجتماعية و الخصوصية

أ– تعريفها

يمكن تعريف الشبكات الاجتماعية، على انها مواقع على الإنترنت، يتواصل من خلالها ملايين البشر، الذين تجمعهم اهتمامات أو تخصصات معينة، ويتاح لأعضاء هذه الشبكات، مشاركة الملفات والصور، وتبادل مقاطع الفيديو، وإنشاء المدونات، وإرسال الرسائل، وإجراء المحادثات الفورية. ويعود سبب وصف هذه الشبكات بالاجتماعية، أنها تتيح التواصل مع الأصدقاء وزملاء الدراسة، وتقوي الروابط بين أعضاء هذه الشبكات في الفضاء السيبراني. وتتنوع الشبكات الاجتماعية على الانترنت، بتنوع الهدف من انشائها. فمنها المهنية، ومنها العلمية، ومنها الاجتماعية. ولكن يمكن تقديمها جميعا، انطلاقا من تركيبتها، كمجموعات من الأشخاص والمؤسسات أو الهيئات، التي تبني فيما بينها علاقات مباشرة أو غير مباشرة، بناء على وحدة الاهتمامات، أو النشاطات المهنية والثقافية، أو الروابط الاجتماعية الاخرى، سواء كانت سياسية أو دينية أو عائلية. ومن أشهر الشبكات الاجتماعية في العالم: فيس بوك (Facebook.com)، وتويتر (Twitter.com)، وماي سبيس (myspace.com) وغيرها[272].

ب– استخداماتها

وتتيح هذه الشبكات لاعضائها، امكانية التواصل المباشر والفوري، فيما بينهم، دون اي مقابل مادي، ودون اي تعقيدات على مستوى اصول وشروط التسجيل، الامر الذي يشجعهم على استخدامها، للوصول، ليس إلى الاصدقاء والاقارب فقط، بل إلى اوسع شريحة من مستخدمي الانترنت.

[272] *Bebo, Classmates.com, Delicious, Digg, Facebook, FriendFeed, Friendster, Hi5, Last.fm, LinkedIn, LiveJournal, MySpace, Ning, Reddit, Slashdot, StumbleUpon, Tagged, Twitter*

كذلك، يمكن لمستخدمي هذه الشبكات، إنشاء مدوناتهم الخاصة، حيث يناقشون القضايا التي تثير اهتمامهم، وحيث يمكنهم ان يحشدوا لدعم رأي ما، أو لمعارضة موقف وراي آخر. وغالبا ما يسعى مستخدمو هذه الشبكات، إلى بناء شبكة من العلاقات، أو مجموعات، ينشر اعضاؤها معلومات شخصية عن اهتماماتهم، وهواياتهم، كما عن وضعهم العائلي، والمهني، والأكاديمي، وخلفياتهم الثقافية، والدينية، والسياسية.

وإذا كان العديد من هذه الشبكات، يسمح بتحديد نوع وكمية المعلومات، كما حلقة الأشخاص الذين يمكنهم الاطلاع عليها، فان الوصول إلى هذه المعلومات، واستغلالها باي شكل من الاشكال، يبقى ممكنا، ويبقى استثمارها أحد اهم الأهداف، التي تقف وراء جمعها، وذلك بغض النظر عن الاسباب الكامنة وراء ذلك، اقتصادية كانت، ام اجتماعية، ام أمنية.

كذلك، يمكن استخدام هذه الشبكات، لأهداف مهنية بحتة، سواء لمتابعة وتوسيع الجهود والآفاق المهنية، أو لتبادل الآراء حول موضوع معين، أو لطلب المساعدة من الزملاء الأكثر اطلاعا وخبرة.

ولا يعتبر الوصول إلى هذه الشبكات، حكرا على مستخدمي الانترنت، ذلك انه متوافر أيضا على اجهزة الاتصال الخليوية، وعلى البلاكبيري، وغيرها. وتترك هذه الشبكات، أثرا أساسيا في الحياة اليومية لملايين الأشخاص حول العالم، يشكل الشباب، شريحة هامة منهم. ولعل أهم المؤشرات، على ذلك الأثر، هو اهتمام رجال الأعمال، كما الشركات، ليس فقط بما ينشر وينفذ من دراسات حول مستخدمي الانترنت، والشبكات، بل وإضافة إلى ذلك، بتدريب وتعليم المهنيين، على كيفية التعامل مع الانترنت، ومنهجيات وأساليب إيجاد حيثية ومصداقية، تخدم تطورهم المهني، والمالي.

ويبقى العنصر الأكثر اجتذابا للمنضمين إلى الشبكات الاجتماعية، هو التواصل الاجتماعي، ما يعني عمليا، تبادل كمية أكبر، من المعلومات الشخصية[273].

من هنا، تعتبر الشبكات الاجتماعية في "الفضاء السيبراني"، البيئة الأخطر على الحق في الخصوصية، كونها الأكثر استنزافا للبيانات الشخصية، والأكثر تحريضا للشباب على الاستعراض، وعلى توسيع دائرة انتشارهم، كما انها المواقع التي تجتذب العدد الأكبر، من زائري الفضاء السيبراني[274].

ولعل الاعداد الهائلة، لمستخدمي هذه الشبكات، تجعلنا ننتبه إلى حجم المعنيين باستقرار الفضاء السيبراني، وبما يجري فيه، وبما يمكن ان ينتج من عدم استقراره. كذلك، لا بد من الانتباه إلى الإمكانات الواسعة التي يتيحها، وتأثيرها في المجتمعات المختلفة، تبعا لطريقة استخدامها من قبل الأفراد. وكان البعض، قد نسب نجاح عدد من الثورات في المنطقة العربية، كما بعض الاضطرابات التي حصلت، إلى التجييش والحشد، والتواصل، الذي كان يتم بين المجموعات التي تتلاقى على أهداف واحدة، أو

[273] *Sarah Perez. More Adults Than Ever on Social Networks.http://www.readwriteweb.com/archives/more_adults_than_ever_on_socia.phpIt appears that the trend of using social networking sites for professional purposes is not quite as common as we may have thought. Although there are portions of the population both young and old that do so, it isn't the main reason people join social networks. It's more common for people to go online to use the networks as they were originally intended - to socialize.*

[274] *http://blog.nielsen.com/nielsenwire/online_mobile/social-media-accounts-for-22-percent-of-time-online/ June 15, 2010- The popularity of social media is undeniable – three of the world's most popular brands online are social-media related (Facebook, YouTube and Wikipedia) and the world now spends over 110 billion minutes on social networks and blog sites. This equates to 22 percent of all time online or one in every four and half minutes. For the first time ever, social network or blog sites are visited by three quarters of global consumers who go online, after the numbers of people visiting these sites increased by 24% over last year. The average visitor spends 66% more time on these sites than a year ago, almost 6 hours in April 2010 versus 3 hours, 31 minutes last year.*

التي يمكن تحريكها، حول قضية معينة. ولذا يمكننا وصف الانترنت، في جانبها الايجابي، ووسائل التواصل الاجتماعي، بمحركات التطور والحرية والديمقراطية. اذ انها تفتح الآفاق على المعرفة، وعلى الاتصال بالآخر المختلف، وعلى التدرب على فكرة وجود شيء مختلف. وسواء اكان ذلك صحيحا ام لا، فان الأكيد هو تلك القوة، التي تمنحها التقنيات للأفراد وللمجموعات، على السواء. ولا تخرج الدولة عن هذه القاعدة، اذ تمنحها التقنيات الحديثة امكانات هائلة، هي الاخرى للقمع [275]، حيث تتحول البنية التحتية المركزية وعالية التقنية، بسهولة فائقة، إلى أداة في يد الحكومة، لممارسة رقابتها. و لم تقف الحكومات القمعية عاجزة، امام واقع إدارة القطاع الخاص، للجزء الأكبر من هذه البنية، اذ فرضت شروطا قاسية على الشركات، جعلتها تذعن لطلبات الحكومة. من هنا القول، بان الرقابة عملية تتم بالتعاون بين القطاعين العام والخاص.

على المستوى القانوني، يثير استخدام الشبكات الاجتماعية، عددا من المسائل، التي تدور، بشكل أساسي، حول اساءة استخدام المحتوى، والاثبات، والتشهير، إضافة إلى دور ايجابي لها، كونها تشكل أرضية خصبة، تتيح إمكانات هائلة أمام الأجهزة الأمنية، والسلطات الرسمية، لجمع الأدلة، وملاحقة المجرمين.

ج- إشكالية الموافقة والمعالجة

ترتكز آلية حماية البيانات الشخصية، في معظم القوانين، على عدد من المبادئ، يأتي في مقدمها: حظر جمع المعلومات ومعالجتها، الا لهدف شرعي محدد ومعلن، لا يجوز الحياد عنه، الا بموافقة صاحب المعلومات.

وعليه، تطرح البيانات الشخصية على الشبكات الاجتماعية إشكالية خاصة، تتمثل في قيام صاحب البيانات شخصيا بتحميلها على الموقع، وبعرضها على الانترنت، مع موافقته على سياسة، أو قواعد الخصوصية التي تعتمدها الشبكة، أو الموقع. وهذا يستدعي أولا الانتباه، إلى أن الغالبية العظمى من مستخدمي الشبكات، لا يقرأون الاتفاقيات التي يوقعون عليها، أو لا يفهمونها تماما. وبالتالي، فان معالجة المعلومات وحفظها، استنادا إلى موافقة صاحب العلاقة، تثير الشكوك حول مشروعيتها، طالما لم يتمكن المستخدم من استيعاب امكانات وأساليب وأهداف المعالجة، التي يمكنها ان تتعدد وتتشعب بما يخرج عن سيطرته، وربما عن سيطرة الموقع نفسه. أما ثانيا، فيفترض البحث، عن مدى امكانية معرفة الهدف، الذي تجمع لاجله المعلومات، وتحديد شرعيته، وآلية ضبط الالتزام به.

على مستوى آخر، وبالعودة إلى النصوص القانونية، نتوقف عند غياب الاحكام القانونية الخاصة بحماية المعلومات الشخصية على الشبكات الاجتماعية، حتى في دول الاتحاد الأوروبي، بالرغم من ريادة هذه الأخيرة، في مجال حماية المعلومات الشخصية، والحياة الخاصة. فقد اهتم القانون بحماية الخصوصية، والبيانات الشخصية، ضد مستغليها من مجرمين، أو تجار، أو مستثمري معلومات، أو إدارة تميل إلى اساءة استعمال حقها، وسلطتها، بما يعرض هذه الحقوق والحريات للمخاطر. الا انه، لم يهتم

---

[275] * *Social media — tool of revolution or repression? https://ethics.journalism.wisc.edu/2011/01/31/social-media-tool-of-revolution-or-repression/*
* *The new media: Between revolution and repression – Net solidarity takes on censorship. https://rsf.org/en/news/new-media-between-revolution-and-repression-net-solidarity-takes-censorship*

أبدا بحمايتها، ضمن إطار العلاقات الاجتماعية، وفي سياق نشرها من قبل المعني بها، واغفاله تدابير الحيطة التي يستدعيها الحفاظ على حقه في الخصوصية، وسلامته.

في هذا السياق، ونتيجة الانعكاسات السلبية، التي يمكن ان يتركها استغلال البيانات الشخصية بطريقة غير شرعية، أو بطريقة ترتب مسؤولية على الأشخاص والشركات المعنية بمعالجتها، لجأت المواقع المختلفة، إلى وضع اتفاقية للخصوصية، تكاد تصبح جزءا أساسيا وبديهيا، من أي موقع على الانترنت. وغالبا ما تحتوي هذه الاتفاقية، التي يوافق عليها المستخدم، معلومات عن وسائل وأساليب استخدام البيانات، التي تحمل على الموقع. كما تحتوي على تفاصيل، حول الجهات التي يمكن ان تستفيد منها، أو ترسل اليها. إضافة إلى ذلك، يمكن ان تشير إلى استخدام الكعكات، التي تساعد على رصد المستخدم. اما فعالية هذه الاتفاقية، فوقف على القوانين التي تخضع لها. والفرق أكثر من شاسع، كما هو معلوم، بين الأنظمة القانونية، التي سيتم الاحتكام اليها، في حال الخلاف. فبين النظامين الأوروبي والأميركي مثلا، تختلف قواعد واصول حماية البيانات الشخصية، وامكانية الوصول اليها. وهذا ما دفع محرك البحث "غوغل"، إلى المطالبة بإيجاد معايير عالمية واضحة، لحماية الخصوصية.

الا ان الأساس في الحماية، يبقى مرتكزا إلى مدى وعي المستخدم، وقدرته على استخدام التقنيات الخاصة بحماية الخصوصية، التي تتيحها المواقع، لاسيما متى كان المبدأ هو الانكشاف على اوسع جمهور ممكن، بينما اخفاء المعلومات، هو ما يجب ان يختاره المستخدم. فاستخدام البيانات الشخصية، مرتبط بالسمعة، والأمن، والخصوصية، وبالتالي بالعديد من الحريات والحقوق المدنية.

ومع الحوسبة السحابية، يمكن الاطلاع على المعلومات، من اي مكان في العالم. فمحركات البحث تخضع لقانون البلد، الذي تستقر فيه. فغوغل مثلا، وانسجاما مع قانون [276] مطبق في الولايات المتحدة الأميركية، لا بد له، من كشف اسم صاحب الحساب، وبياناته، وسجل دخوله إلى الgmail. ويبقى هذا حريا بالانتباه، وان ترافق مع حق محرك البحث، في عدم الاستجابة، الا بموجب مذكرة صادرة عن السلطات القضائية المختصة، في حال طلب معلومات اضافية، أو حقه في طلب مذكرة تفتيش وتحر، في حال تضمن الطلب، الاطلاع على محتوى البريد الإلكتروني.

على مستوى قانوني مكمل، تشكل البيانات الشخصية في الفضاء السيبراني، هوية، تعود مسؤولية الحفاظ عليها إلى مالكها، تماما كما تعود اليه مسؤولية حماية هويته في العالم المادي، وعدم السماح لآخر باستخدامها. فاذا كان الحفاظ على الاوراق الثبوتية، كبطاقة الهوية وجواز السفر، وغيرها، من واجبات مالكها، ومسؤوليته، فان المحافظة على البيانات الشخصية في الفضاء السيبراني، هي من واجبات ومسؤولية من تعود اليه، بغض النظر عن مكان وجود أو تخزين هذه المعلومات. وإذا كانت سرقة الاوراق الثبوتية في العالم المادي، تشكل خطرا على صاحبها، لاسيما استخدامها لتنفيذ أعمال جرمية، فان سرقة البيانات الشخصية، يمكنها ان تؤدي هي الاخرى، إلى انتحال هوية، لارتكاب اعمال جرمية. مع الإشارة هنا، إلى الإشكالية الاخرى، التي تثيرها، مدى قدرة صاحب البيانات الشخصية على المحافظة عليها، في بيئة عالية التقنية، حيث يعجز بعض الاختصاصين، عن حماية أنظمتهم المعلوماتية، أحيانا كثيرة، من خطر الاقتحام، والتلاعب بالبيانات. كما تثار هنا إشكالية

[276] *subpoena*

خاصة تتناول أساس المسؤولية، فهل هو الخطأ، أم التقصير، أم الاهمال؟ للاجابة على هذا السؤال، لا بد من التوقف عند وعي مستخدم الانترنت للمخاطر، وقدرته على مواجهتها، كما لا بد من التوقف، عند دور السلطة، في نشر الوعي حول هذه المخاطر، وفي تمكين المستخدمين، وتأمين الاطر التنظيمية والقانونية لحمايتهم.

٥. وسائل الحماية

تتكون وسائل حماية البيانات الشخصية، بالإضافة إلى التوعية، من إجراءات تقنية وقانونية. لكننا سنحصر بحثنا، في هذه الوسائل، على الوسائل التشريعية والتنظيمية، نظرا لدورها الأساسي، حتى في تقرير الحماية التقنية نفسها، عندما تفرضها، وتنظم المحاسبة عن عدم الالتزام بها.

ويتناول التشريع في مجال حماية البيانات الشخصية، مجالات: الحريات والحقوق الأساسية، الأمن والعدالة، التقنيات والإجراءات المطلوب الالتزام بها. ويرتبط تنظيم الفئة الأولى من الحماية، بالاستخدامات الخاصة وبالممارسات التجارية، بينما يرتبط تنظيم الفئات الاخرى، بترتيب علاقات الأفراد مع الدولة، وعلاقات ادارات الحكومة فيما بينها، لاسيما منها الهيئات المتخصصة في ملاحقة الممارسات، والأعمال المخالفة للقوانين، والمخلة بالأمن. وهذا يعني، وجود قواعد منشئة أو مقرة للحقوق، والموجبات، والحريات، وكيفية الحفاظ عليها، في مواجهة معالجة البيانات الشخصية، بطريقة تعرض هذه الحقوق. كما يعني هذا أيضا، وجود قواعد أخرى خاصة، تلحظ الحالات والاستثناءات التي تبرر معالجتها، وتبادلها ونقلها، خارج القواعد المعمول بها للحماية. ويطرح هذا الامر، ضرورة رفع التحدي، الخاص بإيجاد التوازن بين الحماية، وحقوق وحريات اخرى، منها ما يتعلق بالأفراد الآخرين في المجتمع، وحرياتهم، مثل: حرية التعبير، وحرية تبادل البيانات، والحق في الوصول إلى المعلومات، ومنها ما يتعلق بحقوق المؤسسات التجارية، في إدراة هذه البيانات وجمعها، والافادة منها في نشاطها الاعتيادي، ومنها الآخر، ما يتصل بواجبات الدولة في حماية السلامة العامة والأمن القومي، والتي لطالما ارتبطت، بجمع المعلومات، وتبادلها، والوصول اليها.

أ- دليل توجيهي ومبادئ

ينطلق التشريع لحماية البيانات الشخصية، على المستوى الدولي، مما يمكن اعتباره، إطارا عالميا للحريات الشخصية، وهو شرعة حقوق الإنسان الصادرة عن الأمم المتحدة ١٩٤٨، التي اقرت في المادة ١٢ "حق الشخص بعدم التعرض الاعتباطي لخصوصيته وحقه في حفظ كرامته وحقوقه الفردية". ويندرج في هذا السياق، الاهتمام في انحاء العالم، بالحفاظ على البيانات الشخصية، كخطوة ضرورية، للحفاظ على الحق في الخصوصية[277].

وكانت منظمة التعاون الاقتصادي والتنمية، قد أصدرت دليلا حول حماية الخصوصية، وتوصية للدول الأعضاء بالالتزام به. وقد لعب هذا الدليل، دورا أساسيا في التوجهات التشريعية للدول الأوروبية، وتضمن عددا من المبادئ هي: محدودية عمليات جمع البيانات Collection-limitation،

[277] مؤتمر استوكهولم ١٩٦٧ - مؤتمر طهران ١٩٦٨ باشراف الأمم المتحدة

نوعية البيانات Data quality، وتحديد الهدف Purpose-specification، وحصر الاستخدام بالهدف المحدد Use-limitation، وتأمين وسائل حماية وأمن المعلومات Security-Safeguards، والعلانية Openness، والحق في المشاركة والمساءلة Individual Participation and Accountability. وتقتصر تغطية هذا الدليل، على البيانات الخاصة بالأشخاص الطبيعيين، المعالجة آليا، أو يدويا، في القطاعين العام والخاص. كما تبنت الأمم المتحدة، عام ١٩٩٠، من خلال هيئتها العامة، دليلا لتنظيم المعالجة الآلية للبيانات الشخصية، تضمن مبادئ الدليل، الذي أصدرته منظمة التعاون الاقتصادي والتنمية. ويمثل هذا الدليل، توصية للدول الأعضاء، بضرورة تبني تشريعات تنظم معالجة البيانات الشخصية.

ب- قوانين وإرشادات

في العام ١٩٧٨، صدر قانون فرنسي حول حماية البيانات الشخصية، تحول إلى أداة عمل في اتفاقية المجلس الأوروبي الصادرة عام ١٩٨١. بعد ذلك، صدر الارشاد الأوروبي عام ١٩٩٥، أي بعد صدور توجيهات منظمة التعاون الاقتصادي والتطوير، عام ١٩٨٠، وذلك، بهدف منع التناقض وعدم الانسجام، بين القوانين الأوروبية الخاصة بحمايات البيانات الشخصية، مما يمكنه ان يؤثر سلبا على التجارة الإلكترونية، والخدمات بين دول الاتحاد.

وبالفعل، فقد أرسى هذا الارشاد، مبادئ عامة وقواعد واضحة، يمكن الركون إليها والاسترشاد بها، لاسيما وانه قد جاء خاليا من أي تفاصيل اجرائية، يمكن ان تعرقل عملية التطبيق، ومؤسسا لإنشاء سلطات وطنية للرقابة. وكان الهم الأساس من هذا الارشاد، هو الحفاظ على الحريات الشخصية، واحترام حقوق الإنسان، ضمن البيئة الجديدة. وبالفعل، فقد شكل ارشاد العام ٩٥، نواة الحركة التشريعية الأوروبية، الهادفة إلى حماية البيانات الشخصية. وقد أدخل هذا الارشاد، مصطلحات جديدة، "كالبيانات الشخصية"، و"معالجة البيانات الشخصية"، و"مراقب المعالجة"، و"المعالج"، و"المتلقي"، و"أصحاب البيانات". واقتصر تطبيق هذا الارشاد، على معالجة البيانات الشخصية، التي تجري ضمن الاتحاد الأوروبي، والتي تخضع لقوانينه، مستثنيا عمليات المعالجة الخاصة بالسلامة العامة، والدفاع، وأمن الدولة، ونشاطات الحكومة، في المجال الجزائي.

وقد تبع هذا الارشاد، ارشادات وقرارات لاحقة، احتفظت بالمبادئ العامة، واضافت ما يتماشى مع مستجدات المعالجة الإلكترونية، ونقل البيانات، لاسيما فيما يتعلق بأساليب المعالجة، وطرق النقل.

ونورد في هذا المجال، اتفاق الملاذ الأمن، الموقع بين الاتحاد الأوروبي، والولايات المتحدة الأميركية، والذي يوجب على كل شركة، راغبة في تلقي بيانات شخصية من إحدى دول الاتحاد الأوروبي، ان تلتزم مستوى حماية ملائمة للارشاد رقم EC/٤٦/٩٥. كذلك الارشاد الصادر، عام ٥٨/٢٠٠٢، والمعدل في العام ٢٠٠٨، حول الخصوصية الإلكترونية، والإطار التنظيمي لعمل المجلس للعام ٩٧٧/٢٠٠٨ تاريخ ٢٧ تشرين الأول – نوفمبر، حول حماية البيانات الشخصية في مجال العمل التعاون القضائي، والأمني. وينظم هذا الإطار، بعض الحقوق، مثل إعلام صاحب البيانات، والوصول إلى البيانات المحفوظة لدى الأجهزة الأمنية المعنية بالملاحقة والتحقيق، والتعويض في حال المعالجة

مخالفة للقانون، والقيود الموضوعة على معالجة البيانات الشخصية. وينحصر مدى تطبيقه، على البيانات الخاصة بالشؤون الأمنية والعسكرية، التي يتم تبادلها بين دول الاتحاد، دون تلك التي تتم معالجتها، على المستوى الوطني.

ج- تمايز في اتجاهات التنظيم

لكن الانسجام الذي تحقق على المستوى الأوروبي، وبعض المستوى الدولي، لا يمنع وجود اختلافات وتمايز، ناتجة احيانا عن اختلاف الأنظمة القانونية. ويبدو هذا الاختلاف واضحا، على مستوى بعض المسائل الخاصة بحماية البيانات، مثل: نوعية الأشخاص المعنيين بالحماية (الشخص الطبيعي والشخص المعنوي)، ونوعية المعالجة المقصودة (الآلية أو اليدوية)، والجهات المراقبة، وأصول نقل وتبادل البيانات، والأعمال الجرمية.

وتتوزع اتجاهات التنظيم، على المستوى العالمي، بشكل أساسي، بين تلك التي تنضوي تحت لواء الولايات المتحدة الأميركية، وتلك التي تنضوي تحت لواء الاتحاد الأوروبي، وتلك التي تنضوي تحت لواء الأنظمة القمعية[278]. إلا إن الجميع يخضعه، بشكل أو بآخر، للشروط الخاصة التي تمليها تقنيات الانترنت، والشركات القائمة على تطويرها، مع الإشارة إلى خضوع الشركات التجارية هي الأخرى، إلى الاعتبارات التجارية والاقتصادية التي ترتبط بها، والتي أخضعتها إلى رغبات الأنظمة السياسية وسياستها الخاصة[279]، في مجال الرقابة على الانترنت، والحد من النفاذ إلى المعلومات، واستخدام البيانات الشخصية.

ويطاول هذا الاختلاف، الجهات التي تساهم في التنظيم، وصولا إلى آلياته ومضمونه. ففي أوروبا، تخضع عملية تطوير المقاييس المعتمدة في تكنولوجيا لمعلومات والاتصالات، إلى جهات رسمية، بينما يسيطر القطاع الخاص على هذه العملية، في الولايات المتحدة الأميركية. كذلك، يعكس كل من القانونين: الأوروبي والأميركي، قيما ثقافية مختلفة، عن السلطة العامة، والسوق، ومجالات التشريع والتنظيم.

ويبدو هذا الاختلاف الثقافي واضحا[280]، على مستوى المضمون، كما على مستوى المقاربة، لاسيما في مسألة معالجة البيانات الشخصية، وحماية حق الأفراد في الحفاظ على الخصوصية[281]، حيث يبرز الاختلاف، بدءا من الدستور، اذ تتقدم حرية التعبير على الحق في الخصوصية، بحسب الدستور الأميركي، بينما تتقدم الخصوصية على هذا الحق، في دول الاتحاد الأوروبي، وحيث يتولى الأفراد أنفسهم والشركات التجارية، في الولايات المتحدة الأميركية، مسؤولية تقرير سياسة الحماية الشخصية على الانترنت، إلى حد كبير. ويعتمد في هذا المجال، مبدأ الانضباط الذاتي. ويجد هذا الامر مبرراته، في وجود إطار تشريعي للحماية، يشمل منع المنافسة غير المشروعة، ومنع الاحتكار، وحماية المستهلك، ومنع الغش.

في المقابل، تتولى الدولة، الجزء الأكبر والاشمل من هذه المهمة، في أوروبا، باعتبارها إحدى واجبات

[278] وتأتي في هذه الفئة على سبيل المثال: الصين وبعض البلاد العربية

[279] على الالتزام بمنع الوصول الى بعض المواقع، بناء على رغبة الحكومة الصينية، وبما ينسجم مع النظام السياسي المعتمد من yahooو microsoftو googleموافقة قبل هذه الاخيرة

[280] *"While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacyfrom that taken by the European Union", Safe Harbor Principles.*

[281] من التفسيرات التي يمكن ان تساق في هذا المجال، هو ميل الأنظمة التي تعتمد النظام العرفي الى التركيز بنسبة أكبر على العلاقة، بين القانون والاقتصاد والمجتمع، بينما تميل الثانية، الى التركيز أكثر، على العلاقة ،بين القانون والسياسة والمجتمع

السلطة في حماية المواطنين، دون اسقاط مبدأ المشاركة في الضبط، والذي يعني مساهمة القطاعات المعنية، التجارية منها والمدنية[282]. وتعمل هيئات الاتحاد الأوروبي، على توجيه الدول الأعضاء، إلى اصدار تشريعات، تتلاءم مع القواعد المقررة في التوصيات الصادرة عن منظماته: كمجلس أوروبا، واللجنة الأوروبية، والاتحاد الأوروبي. كما يبرز الاتجاه الأوروبي بوضوح، نحو التنظيم التشريعي الشامل، عبر قوانين البرلمان الأوروبي.

د- اتفاق الملاذ الأمن

أبرز الاختلاف في التنظيم، خطورته على حماية البيانات الشخصية، ما أدى إلى تهديد الاتحاد الأوروبي، بحظر انتقال البيانات الشخصية، إلى البلاد التي لا تؤمن معايير حماية ، موازية لتلك المعمول بها، في التوصيات الصادرة عنه[283]، وذلك انسجاما مع المبادئ التي تقرها هذه الأخيرة، الامر الذي نتج عنه، مشاورات بين وزارة التجارة الأميركية، و اللجنة الأوروبية، لإيجاد آلية تسهل عملية الانتقال هذه، فكان اتفاق الملاذ الأمن:"safe Harbor Agreement".

يضم الاتفاق عددا من المبادئ، التي لا بد من الالتزام بها، من قبل الشركات الأميركية، الراغبة في الافادة، من استمرار دفق البيانات الشخصية اليها من أوروبا. وتتناول هذه المبادئ، ضرورة الالتزام بعدد من الاصول، التي تضمن لحماية الأفراد، إطارا تشريعيا معقولا، يمكن ان يمنع الاعتداء على خصوصيتهم. ومنها:

- موجب الإعلام: اذ يفترض بالشركات، توفير المعلومات التي توضح أهداف جمع ومعالجة بياناتهم الشخصية، وطريقة التصرف بها، لاسيما عندما يتعلق الامر، بنقلها إلى جهة ثالثة. وفي الحالة الأخيرة، يجب اطلاع الأفراد، على طبيعة الجهة الثالثة، التي يمكن أن تحصل على هذه المعلومات، مع اشارتها إلى الخيارات المتاحة، للحد من استخدام هذه البيانات، ومن كشفها. يضاف إلى ذلك، اعطاؤهم المعلومات، حول كيفية الاتصال بالشركة، لنقل أي سؤال، أو شكوى.
- حق الاختيار: اعطاء الأفراد، الحق في قبول أو رفض، كشف أو نقل بياناتهم الشخصية، إلى جهة ثالثة، أو استخدامها، لهدف لا يتناسب مع الهدف الذي جمعت لأجله، والذي تم على أساسه القبول.
- نقل البيانات إلى جهة ثالثة: في هذه الحال، تلتزم الشركات موجب الإعلام الواضح، كما تلتزم تأمين الخيارات. بالإضافة إلى ذلك، يتوجب عليها، أن تتأكد من أن التزام الجهة الثالثة، اتفاق الملاذ الأمن، أو التوصية الأوروبية لحماية البيانات الشخصية، أو أي سياسة حماية أخرى، مناسبة تحل محله. كما يمكن، أن تتفق الشركة، مع الجهة الثالثة، على احترام مستوى الحماية المطلوب.
- حق النفاذ: اعطاء الأفراد حق النفاذ إلى البيانات الشخصية التي تجمع عنهم، لتصحيحها، وتعديلها، أو الغائها، حين لا تكون صحيحة. ويمكن السماح للجهة التي تجمع البيانات، بعدم اعطاء هذا الحق للمعنيين بالبيانات، في حال كان هذا النفاذ، ذا كلفة مرتفعة، لا تتناسب وحجم

[282] *Law put to the test by information technologies. Interviews with French parliamentary Deputy Christian Paul, and Olivier Debouzy.www.france.diplomatie.gouv.fr- on the amerrican side, the individuals active on the web intend to regulate their activities themselves. On the French side, the concept of co-regulation is being promoted by the combined forces of business, users and the authorities.*

[283] *The "safe Harbor Agreement" formula., was suggested by US Ambassador Aaron. Safe Harbor Privacy Principles issued by the U.S. Department of Commerce on July 21, 2000*
بحسب هذا الاقتراح، يمكن للشركات الأميركية التي تتعاطى معالجة المعلومات الشخصية، أن تلتزم القواعد المعمول بها في الاتحاد الأوروبي حول حماية المعلومات الشخصية

المخاطر التي يتعرض لها الفرد، أو في حال كان نفاذه إلى هذه البيانات، يتعرض لحق الآخرين في الخصوصية.

- أمن المعلومات: تلتزم الشركات، موجب حماية البيانات. ويفترض بها، اتخاذ الإجراءات الكفيلة، بمنع تعريضها للضياع، أو اساءة الاستعمال، أو الانكشاف، أو التشويه، أو التلاعب بها.
- مصداقية البيانات Data integrity يجب أن تتناسب البيانات الشخصية، مع الأهداف التي ستستخدم لأجلها. ويفترض بالشركة اتخاذ الخطوات المعقولة، لضمان مصداقية البيانات، وصحتها.
- التطبيق: تلتزم الشركات إيجاد آلية، تسمح بالنظر في شكاوى الأفراد، وحل النزاعات، وتقرير التعويضات حيث يجب، وبمقتضى القواعد القانونية. إلى جانب ذلك، يجب توفير اصول خاصة، لمراقبة مدى التزام الشركات، وتنفيذها للخطوات المطلوبة، كشرط لقبول انضمامها، وفرض عقوبات شديدة، على مخالفة هذه الالتزامات، كالشطب من لائحة الشركات، التي تستفيد من الاتفاق، مثلا.

هذا، ويعود قرار الانضمام إلى الاتفاق، إلى الشركات نفسها، التي يفترض بها، أن تعلن التزامها بتطبيق شروطه، وتحترم هذا الالتزام. ويتم ذلك، بتوجيه رسالة بهذا المعنى، إلى وزارة التجارة الأميركية، كل عام. وتتضمن الرسالة الإعلان، والخيار، والنفاذ، والتطبيق[284]. ويفترض بالشركة، التي ترغب في الافادة من هذا الاتفاق، أن تعلن عن انضمامها اليه، وذلك في سياسة الحماية التي تنشرها على موقعها.

ويشترط لقبول انضمام هذه الشركات إلى الاتفاق، أن يكون لديها سياسة حماية، خاصة بالبيانات الشخصية، سواء عبر انضمامها إلى أحد برامج الحماية، الملتزم بالاتفاق، أو عبر تطويرها لبرنامج خاص بها، يتناسب ومندرجات التوصية الأوروبية.

هـ- الإطار التشريعي اللبناني

لا يوجد في لبنان نص خاص، لحماية المعلومات الشخصية. ولكن يسجل له، انه يؤمن سندا دستوريا للحقوق والحريات الأساسية، التي يمكن ان يمس بها الاعتداء على الحريات الفردية، وفي مقدمها، الحق في الخصوصية. وتتوزع الاحكام ذات العلاقة، على الدستور من جهة، وبعض القوانين الوضعية اللبنانية، من جهة أخرى.

- الدستور

يمكن القول، ان الأساس لحماية البيانات الشخصية، في لبنان، هو دستوري[285]. فالدستور اللبناني، يعلن في مقدمته، عن التزام الشرع الدولية، والاتفاقات العالمية، الخاصة بحقوق الإنسان، وذلك دون اي تمييز بين ابنائه. كما يعتبر احترام الحريات العامة والحقوق، من ركائز الجمهورية الديمقراطية البرلمانية، وفي مقدمها، حرية المعتقد والرأي، والعدالة الاجتماعية والمساواة. ويبدو واضحا، ان الدستور اللبناني، يتعامل مع الخصوصية ببعدها المادي، من خلال إقراره حرمة المنزل، والحرية الشخصية، واحترام

[284] *Includes elements such as notice, choice, access, and enforcement.*
[285] الدستور: تنص المادة الرابعة عشر على ما يلي: للمنزل حرمة لا يجوز لأحد الدخول اليه الا في الأحوال والطرق المبينة في القانون

الملكية. الا انه يتعامل معها أيضا ببعدها غير المادي، عندما يقر حرية الراي والمعتقد، وحرية التعبير عن الرأي. علما انه يضع حدودا لهذه الحريات، هي النظام العام والآداب، واحترام حقوق الآخرين. وقد اقرت المادة الثامنة، مبدأين أساسيين في حماية الحريات والحقوق هما: مبدأ شرعية الجرائم والعقوبات، ومبدأ خضوع الإجراءات التي تمس بالحرية إلى القانون. ويعزز الاحتكام إلى القانون وسلطته، مبادئ أخرى، مثل مبدا دستورية القوانين، والفصل بين السلطات. وعليه، يصبح تدخل السلطة ممكنا، عندما تسمح بذلك النصوص القانونية، بهدف حماية الأمن القومي، والمصلحة العامة، والنظام الاجتماعي، والاقتصادي، والاخلاقي، والصحة العامة، والآداب العامة.

ويمثل ذلك، على مستوى البيانات الشخصية، إقرارا بحق المواطن، في الحفاظ على بياناته الشخصية، بما يضمن حماية حقه في الخصوصية، من جهة أولى، كما يعني إقرارا بحق الدولة في الاطلاع عليها، ومعالجتها، بما يسمح للسلطات المختصة، بمنع وقوع اعمال مخلة بالأمن والنظام، أو بملاحقة ومعاقبة مرتكبيها، من جهة ثانية.

ـ القوانين الوضعية

في لبنان، لا يوجد نص يحكم مباشرة حماية البيانات الشخصية، وذلك بالرغم من عدد من المشاريع التي قدمت إلى المجلس النيابي منذ العام ٢٠٠٤، وما زالت اللجان حتى اليوم تناقش مشروعا حول المعاملات الإلكترونية وحماية البيانات ذات الطابع الشخصي[286].

لكن المشترع اللبناني، لم يتوان عن إقرار قانون خاص، بحماية الحق في الخصوصية في مجال الاتصالات، بعد ان تعالت الاصوات، مطالبة بحماية الحق في الخصوصية، وحماية الحريات، وبعد سلسلة من الاحتجاجات والاعتراضات، من أكثر من جهة وطرف. فبيانات الاتصالات، نوعان: الأول خاص بعمليات الاتصال، والثاني خاص بالأشخاص الذين يجرون الاتصال. وفي النوعين، يمكن حصول إعتداء على الخصوصية، حيث تسمح الأولى بتحديد الأشخاص من خلال ارقام الهواتف، التي تتم متابعة حركتها، بينما تسمح الثانية، بمعالجة بيانات شخصية، والاطلاع على أمور شخصية.

وقد عرف هذا القانون، بقانون "صون الحق بسرية المخابرات التي تجري بواسطة اية وسيلة من وسائل الاتصال"[287]. وقد تطرق في المادة الأولى[288] منه، إلى حماية التخابر باية وسيلة من وسائل الاتصال، معددا البريد الإلكتروني من ضمن هذه الأخيرة، ومؤكدا على الاهتمام بحماية الحياة الخاصة، والحريات. وكانت المادة التاسعة، أعطت للدولة، في حالات محصورة جدا، حق المراقبة والتتبع، عندما يتعلق الامر بجمع معلومات ترمي إلى مكافحة الإرهاب، والجرائم الواقعة على أمن الدولة، والجرائم المنظمة[289].

[286] دراسة المواد العالقة في مشروع قانون المعاملات الإلكترونية - *http://www.lebanondebate.com/news/247699*

[287] قانون ١٤٠ تاريخ ٢٧ تشرين الأول ١٩٩٩ معدل بالقانون ١٥٨ تاريخ ٢٧ كانون الأول ١٩٩٩

[288] المادةالأولى: الحق في سرية التخابر الجاري بأي وسيلة من وسائل الاتصال السلكية واللاسلكية (الأجهزة الهاتفية الثابتة، الأجهزة المنقولة، والفاكس والبريد الالكتروني...) مصون وفي حمى القانون ولا يخضع لاي نوع من أنواع التنصت او المراقبة او الاعتراض او الافشاء الا في الحالات وبواسطة الوسائل التي نص عليها هذا القانون ويحدد اصولها

[289] المادة ٩ من قانون ١٤٠ تاريخ ٢٧ تشرين الأول ١٩٩٩ معدل بالقانون ١٥٨ تاريخ ٢٧ كانون الأول ١٩٩٩: «لكل من وزير الدفاع الوطني ووزير الداخلية ان يجيز اعتراض المخابرات بموجب قرار خطي معلل وبعد موافقةة رئيس مجلس الوزراء، وذلك في سبيل جمع معلومات ترمي الى مكافحة الارهاب، والجرائم الواقعة على أمن الدولة، والجرائم المنظمة. يحدد القرار وسيلة الاتصال موضوع الإجراء، والمعلومات التي يقتضي ضبطها، والمدة التي تتم خلالها عملية الاعتراض، على ان لاتتجاوز هذه المدة الشهرين وعلى ان لا تكون قابلة للتمديد الا وفقا لاصول والشروط عينها

وكان قانون الدفاع الوطني اللبناني[290]، قد أقر هو أيضا، استثنائيا، وبصورة حصرية (في حالات تعرض الوطن أو جزء من اراضيه أو قطاع من قطاعاته ام مجموعة من السكان للخطر)، حق السلطة في مراقبة الاتصالات، وانما بموجب مراسيم تتخذ في مجلس الوزراء، وبناء على طلب من المجلس الاعلى للدفاع. علاوة على ذلك، حددت المادة ٨٥٠ من قانون العقوبات، عقوبة من شهرين إلى سنتين، لكل شخص ملحق بمصلحة البريد والبرق والهاتف، يطلع بصفته هذه، على مراسلات أو مخابرات غير موجهة اليه. وتنزل نفس العقوبة به أيضا، فيما لو أفشى مضمونها.

وفي السياق عينه، تنص مواد من قانون العقوبات اللبناني، على احكام خاصة ب"الجرائم الواقعة على الحرية والشرف"، وتلحظ عقوبات تطال الأعمال التي تقع ضمن دائرة "افشاء الاسرار": كاتلاف أو كشف رسالة أو برقية، أو كالاطلاع بالخدعة على مخابرة هاتفية[291].

وكان المرسوم ١٥٢٨١، تاريخ ٢٠٠٥/١٠/١، قد نظم عمل الهيئة المستقلة، المكلفة التثبت من قانونية إجراءات الاعتراض الاداري على المخابرات الهاتفية، ومن ثم تولى القانون ١٥٨، تاريخ ١٩٩٩/١٢/٢٧، تعديل القانون ١٤٠، بعد الاعتراض الذي سجل على ضم أعضاء من البرلمان إلى الهيئة، نظرا لما يمكن ان يشكله هذا الامر، من تعارض مع مبدا فصل السلطات، ومبدأ استقلال الهيئة. وقد منحت هذه الهيئة، صلاحيات تحقيق واسعة، تتيح لها عمليا، انجاز مهمتها بالشكل الذي يتناسب ودورها، في صون السرية، والحفاظ على الحريات، حيث يمكنها مساءلة جميع الادارات الرسمية والخاصة، العاملة في المجالات المتصلة بتأمين الاتصالات، وإجراء الكشف الذي ترتأيه، والاستعانة بمن تراه، والاطلاع على المعدات والمستندات اللازمة، بغض النظر عن درجة سريتها.

وفي غياب القوانين الخاصة، تتم معظم الملاحقات المتعلقة بالجرائم المعلوماتية والسيبرانية، امام المحاكم اللبنانية استادا إلى القوانين التقليدية، ومنها قانون العقوبات اللبناني، وقانون المطبوعات. ففي سنة ٢٠٠٠، عرضت على القضاء اللبناني، قضية تتعلق ببث ونشر صور اباحية للأطفال، عبر الانترنت، جرى فيها توقيف المشتبه به، سندا للمواد ٥٣١ و ٥٣٢ و ٥٣٣ عقوبات، التي تجرم التعرض للآداب العامة والاخلاق. وفي قضية أخرى، في العام ٢٠٠٨، تم توقيف بعض الطلاب الجامعيين، ووضعهم قيد الحجز، لمدة أسبوع، في قضية تشهير وتشويه سمعة، نتيجة نشرهم صورا لإحدى الزميلات دون موافقتها، والتعليق عليها بطريقة مسيئة. وكان قانون العقوبات، في مادتيه ٥٣١ و ٥٨٢، هو المعتمد كأساس للتوقيف.

في السياق عينه، وحرصا على حماية مجتمع المعلومات، ومستخدمي الانترنت، انشئ في لبنان مكتب تابع للشرطة القضائية، في قوى الأمن الداخلي، اسندت اليه مهمة مكافحة الجرائم المعلوماتية، والاعتداءات على الملكية الفكرية. وقد تمكن هذا المكتب، بحسب احصاء جرى في العام ٢٠٠٩، من الكشف على ٨٠٪ من الجرائم، التي تقدم المتضررون منها، بشكاوى أمامه.

[290] مرسوم اشتراعي ٨٣/١٠٢ تاريخ ١٩٨٣/٩/١٦
[291] قانون العقوبات اللبناني – الفصل الثاني: «في الجرائم الواقعة على الحرية والشرف" النبذةالرابعة: «في إفشاء الأسرار" المواد من ٥٧٩ لغاية ٥٨١

و- العالم العربي

نقص في التشريع والحماية

يسجل في الدول العربية، نقص واضح في الإطار التشريعي والتنظيمي لحماية البيانات الشخصية، والحياة الخاصة. وإذا كان البعض، يعتبر ان الدستور، إطار ملائم لهذه الحماية، استادا إلى المبادئ والقواعد التي تقر حماية الحريات الفردية، فانه لا يوجد نص دستوري عربي، يقر هذا الحق صراحة،فيما عدا الدستور المصري، الذي أقر في المادة ٤٥، حماية الحياة الخاصة للمواطنين، والدستور القطري (٢٠٠٣)، الذي أقر حرمة خصوصية الإنسان، والدستور التونسي، الذي أقر الحق في الخصوصية[292].

أما القوانين العربية التي يمكن ذكرها، فهي: قانون رقم ٦٣ عام ٢٠٠٤ في تونس، والقانون المغربي رقم ٢٠٠٨-٠٩، وقانون حماية البيانات الشخصية الصادر في الامارات العربية المتحدة عام ٢٠٠٧، وهو قانون خاص بالمركز المالي، صادر باللغة الانجليزية، ومنسجم إلى حد بعيد، مع الارشاد الأوروبي ٩٥، ولكنه أقل شمولية. يضاف إلى ذلك، بعض المواد التي وردت عرضا في بعض القوانين، دون اي تفصيل أو آلية حماية، تضمن تنفيذا فاعلا لها، لاسيما لدى تعارض هذا الحق وهذه الحماية، مع المصلحة العامة وحقوق الغير، كقانون الإحصاءات العامة المؤقت لسنة ٢٠٠٨، الصادر في الاردن، وفيه مواد خاصة بسرية البيانات الاحصائية، ومنع افشائها[293]، وقانون الاتصالات رقم ١٨ الصادر في سوريا عام [294]٢٠١٠، الذي يؤكد على مبدأ احترام الخصوصية. وفي هذا التجاهل لآليات الحماية والتنفيذ، وحدود الممارسة، خطر أكيد، مع تصاعد وتيرة معالجة البيانات الشخصية، وازدياد حجمها، وامكانات معالجتها، واستخدامها، والربط بينها، والتنقيب عنها، بدون معرفة اصحابها وموافقتهم. هذا، ويسجل وجود عدد من مشاريع القوانين، الخاصة بالمعاملات الاكترونية، في الكويت ولبنان وسوريا.

تجدر الإشارة هنا، إلى ان جميع الدول العربية، أعضاء في الأمم المتحدة، وملتزمة الإعلان العالمي لحقوق الإنسان، لاسيما المادة ١٢ منه، التي تقرعدم جواز التدخل التعسفي، في حياة الأفراد الخاصة أو مراسلاتهم، وحقهم في حماية قانونية تضمن ذلك. الا أن آليات التطبيق والتنفيذ، ليست متوافرة لضمان حماية البيانات الشخصية والخصوصية، في غياب قواعد تفصيلية وتطبيقية، لحالات معالجة البيانات، وحفظها، والوصول اليها، وحقوق الأشخاص في المراقبة، والاعتراض، والتصويب، والمحو، وغير ذلك. ومما لا شك فيه، ان هذا الفراغ التشريعي، سيتسبب في تخبط في مواجهة المسائل القانونية، الناتجة عن انتشار معالجة البيانات الشخصية، على جميع المستويات، العامة والخاصة، الداخلية والخارجية، إضافة إلى استمرار جمع وتدفق البيانات عبر الحدود، دون علم اصحابها، واستثمارها واستخدامها، بشكل مناف لحقوقهم.

يضاف إلى ما تقدم، غياب الوعي، لدى العديد من المشرعين العرب، لأهمية حماية البيانات الشخصية، ودورها في تعزيز الانخراط السليم في مجتمع المعلومات، والنمو الاقتصادي والاجتماعي. هذ عدا عن عدم إدراك لخطورة الامر، وعدم قدرة، لدى غالبية مستخدمي وسائل المعلومات والاتصالات الحديثة،

[292] تحمي الدولة الحياة الخاصة، وحرمة المسكن، وسرية المراسلات والاتصالات والمعطيات الشخصية". الدستور التونسي لعام ٢٠١٤
[293] المواد ١١و١٢و٥١و١٦و١٧
[294] المادة ٥٠ من القانون

على حماية أنفسهم، في مواجهة الأخطار والاعتداءات التي تمارس من خلال عمليات معالجة بياناتهم، وتبادلها، ونقلها واستثمارها. ويضاف الى ذلك، انسداد مجالات المراجعة والاعتراض، أمام القلة التي تدرك منهم.

ـ التأسيس على الإطار الدولي

نظرا للبعد العالمي، والعابر للحدود، لحماية البيانات الشخصية، لا بد من الالتفات إلى الاطر، التي يمكن البناء عليها، والانطلاق منها، لاسيما وان لهذه الحماية، ولحماية الخصوصية التي تعنيها، دورا حاسما، في تشجيع التجارة والخدمات الإلكترونية، وفي تحقيق الانسجام، مع توجهات المنظمات والهيئات الدولية، مثل منظمة التعاون الاقتصادي والتنمية والاتحاد الأوروبي، اللذين أصدرا عددا من التوجيهات، والارشادات، والقرارات، في هذا المجال.

من هنا، يمكن الانطلاق في العمل العربي المشترك، من الارشادات التي وضعتها منظمة الاقتصاد والتنمية، حول حماية الحياة الخاصة، وحركة انتقال هذه البيانات عبر الحدود. ويثير هذا الموضوع، مسألتين هما: الشفافية والمسؤولية. ويقوم مبدأ الشفافية بحسب الارشادات، على تأمين الوسائل الكفيلة بتحديد وجود البيانات الشخصية، وطبيعتها، وأهداف معالجتها، ووجهة استخدامها، كما وبتحديد هوية الحائز على هذه البيانات، والمكان الذي يمارس فيه نشاطه. أما المسؤولية، فتعني: ان يحترم الشخص الذي يحتفظ بالمعلومات، القواعد، والإجراءات، التي تضمن تطبيق الارشادات.

وتأسيسا على الانسجام الذي تحقق على المستوى الأوروبي، فيما يتعلق بحماية البيانات الشخصية، وطرق نقلها عبر الحدود، وانطلاقا من الانسجام بين بعض الأنظمة القانونية العربية، التي تنهل من الثقافة الأوروبية، يمكن الافادة من التجربة الأوروبية، في هذا المجال، كنقطة انطلاق إلى تحقيق الحماية والانسجام على المستوى العربي، بالرغم من غياب إطار مؤسساتي عربي جامع، على مثال الاتحاد الأوروبي. كذلك يمكن الافادة، من التفسيرات والجوانب العملية، لكيفية تطبيق الارشاد الأوروبي، والقوانين الأوروبية، والتي أبرزتها القرارات القضائية، الصادرة في مجال حماية البيانات الشخصية، وذلك في إطار تطبيق القوانين الأوروبية، الخاصة بهذا الموضوع.

وقد لجأ معظم المشرعين العرب، الذين وضعوا قوانين في هذا المجال، كما اولئك الذين أعدوا مشاريع قوانين أيضا، إلى النصوص الأوروبية، وغيرها مما هو مطبق. ونذكر هنا، اقتراح القانون اللبناني، حول تنظيم المعاملات الإلكترونية، الذي التزم مبادئ التوصية الأوروبية حول حماية البيانات الشخصية، وأخذ عن تشريعات غربية، واهمها التشريع الفرنسي في هذا المجال، والصادر عام ٢٠٠٤. فقد خصص هذا الاقتراح، المؤلف من ١٧٥ مادة، ٣٠ مادة منه، في الباب الخامس، تحت عنوان "حماية المعلومات ذات الطابع الشخصي"، لحماية هذه المعلومات. وقد توزعت على خمسة فصول، عناوينها الاحكام العامة، وعمليات جمع ومعالجة المعلومات، والإجراءات الخاصة بتنفيذ هذه الأخيرة، وحق الوصول والتصحيح، والاحكام الجزائية التي تطاول مخالفة الاحكام الخاصة بحماية المعلومات.

٦. ضوابط التشريع

تفترض حماية البيانات الشخصية، إحاطة شاملة، بكل الآليات التقنية، ووسائل المعالجة، والتصرف بالبيانات، بحيث لا تترك ثغرات، يمكن النفاذ منها، للالتفاف على الهدف المرجو. وعليه، لا بد لكل إطار تشريعي أو تنظيمي، أو ارشاد، وعلى غرار أي نص قانوني آخر، أو ارشاد أو اتفاقية، ان يلحظ الآتي:

- الأسباب الموجبة، التي تلحظ فلسفة النص، وأهدافه.
- التعريفات الضرورية لوضوح النص ومجال تطبيقه. وعليه لا بد هنا من تحديد: البيانات الشخصية، وعمليات المعالجة، والأنظمة أو الآليات التي يتم العمل بموجبها، إضافة إلى الهيئات والأشخاص المسؤولين والمعنيين، لأهمية تحديد المسؤوليات، في هذا المجال.
- تحديد الجهات التي يمكنها جمع البيانات الشخصية، دون اذن مسبق، على ان تحدد أهداف هذا الاستثناء بوضوح، وعلى أن ينسجم هذا الاستثناء، مع مقتضيات السلامة العامة، والأمن القومي، وطبيعة بعض النشاطات المهنية الخاصة.
- تحديد الشروط التي يمكن على أساسها، الحصول على اذن بمعالجة البيانات الشخصية، ونقلها، وتبادلها، توضح فيه نوعية البيانات التي يمكن معالجتها، أو نقلها، أو تبادلها، كموافقة صاحب البيانات، والمصلحة المبررة والمشروعة، من جمعها.
- تحديد البيانات المستثناة، والاسباب المانعة لمعالجتها، إضافة إلى الحالات التي يمكن فيها تجاوز هذا الاستثناء، شرط الانسجام مع فلسفة النص وأهدافه، أي الحفاظ على حرمة الحياة الشخصية، والحريات الفردية والعامة، والحقوق الأساسية للإنسان، والنصوص القانونية والاحكام، والمصلحة العامة، أو المصلحة الخاصة للشخص المعني، وحرية التعبير.
- إقرار حقوق اصحاب البيانات في الوصول اليها، والتدقيق فيها، وطلب تصحيحها أو محوها، أو منع النفاذ اليها. يضاف إلى ذلك، حق الاعتراض على المعالجة، متى توافرت لدى الشخص اسباب مشروعة، أو متى كان هدف المعالجة، أعمالا تجارية، وترويجية.
- إنشاء هيئات رقابية، ذات صلاحيات للملاحقة والعقاب، تسهر على التطبيق، وحسن سير آليات التنفيذ، بحيث تضمن جميع حقوق الشخص، صاحب البيانات، لاسيما لناحية حقوقه في مراقبة التصرف ببياناته، وأوجه استخدامها، ودقتها، ومصداقيتها، والأهداف التي تستخدم لاجلها. وتدخل في هذا الإطار، الشكاوى، والمراجعات والاعتراضات. من جهة ثانية، لا بد من تنظيم حقوق الجهات المعنية بمعالجة هذه البيانات، سواء أكانت مؤسسات عامة، أم خاصة، أم أشخاصا طبيعيين يستثمرون هذه البيانات، ويديرونها في إطار نشاطهم العلمي، أو التجاري.
- تحديد مسؤوليات الجهات المراقبة وموجباتها، لاسيما لجهة الالتزام بسرية البيانات، والحفاظ على سلامتها وعدم انكشافها، أو تسربها، وتلفها، والتلاعب بها.
- إقرار الحق في التعويض عن المخالفات المرتكبة، واصول مراجعات قضائية وادارية ملائمة، تعزز ممارسة الشخص لحقه في الحفاظ على بياناته الشخصية، ومن خلالها على حريته الشخصية، وحياته الخاصة.
- تأمين حماية البيانات الشخصية المنقولة عبر الحدود، إلى بلد أجنبي، بموجب اتفاقات واضحة، تحترم المبادئ العامة للنص الخاص بالحماية، وفلسفته، على ان تلحظ آليات موافقة وتصريح، لا

تعيق تدفق البيانات لأهداف تخدم تطور التجارة الإلكترونية، والمصلحة العامة، والاقتصاد، والأمن.

- إرساء أخلاقيات خاصة، تجارية ومهنية، وادارية، بالتعامل في مجال معالجة البيانات الشخصية، ونقلها، والتصرف بها، تعزز دور الإطار التشريعي والتنظيمي.
- وضع آليات مواجهة، للتحديات الجديدة التي تفرضها الحوسبة السحابية، لاسيما على المستويات التالية: تشجيع التزام الشركات بقواعد الحماية والأمن، تحديد مسؤولية المتعاقدين مع موفري الخدمة الأساسيين، نوعية الخدمة، طبيعة المسؤوليات، مستويات الحماية، نقل البيانات إلى بلاد، يمكن ان تكون على عداء مع العالم العربي،

٧. خطوات عملية مطلوبة

- إقرار توصية أو ارشاد على المستوى العربي، من خلال جامعة الدول العربية، تتضمن المبادئ العامة لحماية البيانات الشخصية وينسجم مع الاتجاه الدولي في هذا المجال، لجهة الأهداف والفلسفة
- إقرار الاطر التشريعية والتنظيمية الملائمة، على المستوى الوطني
- إنشاء الهيئات الرقابية المناسبة
- وضع أطر تشريعية وتنظيمية، لتبادل البيانات الخاصة بمجالات الأمن والجزاء، بين الدول العربية.
- إنشاء هيئات تنسيق وتعاون عربية، تتولى متابعة التنفيذ على المستوى العربي، والدولي، لاسيما في حالات انتقال بيانات، تخص مواطني أكثر من دولة عربية.
- تعزيز الوعي في المجتمع العربي، بكل قطاعاته المدنية، والمهنية، والحكومية، بأهمية حماية البيانات الشخصية، ودورها في حماية الفرد والمجتمع.
- تنظيم حركة تبادل البيانات الشخصية، بين الدول التي ترغب في حماية بيانات مواطنيها، وتبادل المعارف والخبرات، لفرض حمايتها، استنادا إلى القوانين الوضعية، والى القوانين العربية المشتركة.
- التعاون على إيجاد آليات حماية، تسمح للمواطن بممارسة حقه في الاطلاع على البيانات، وطلب تصحيحها، لدى الدول الاخرى التي تتولى معالجتها، وملاحقة المؤسسات أو الهيئات، التي تمتنع عن تطبيق القوانين الخاصة بالحماية، على غرار ما هو معمول به في مجال ملاحقة المجرمين، ومكافحة الإرهاب، والجرائم العابرة للحدود، بكل أشكالها.

٨. خلاصة

يتبين، على ضوء ما تقدم، ان هنالك حاجة ماسة، إلى إطار قانوني، يضمن تعزيز الثقة في الفضاء السيبراني، وفي استخدام تقنيات المعلومات والاتصالات، عبر ضمان حماية الأفراد، والمؤسسات، والأموال. ولابد لهذا الإطار القانوني، ان يتضمن قانونا خاصا لحماية البيانات الشخصية، وإنشاء هيئة خاصة للمعلوماتية والحريات، تشكل مرجعا لحماية المواطنين وحقوقهم، من كل استثمار غير شرعي في بياناتهم الشخصية، كما ومن كل اعتداء على خصوصيتهم، نتيجة عمليات جمع البيانات،

والتنقيب عنها، وتحليلها، واستثمارها، واي عملية اخرى تطاولها، خارج القواعد القانونية، المرعية الإجراء.

يضاف إلى ذلك، ضرورة الانتباه إلى أهمية توعية المواطنين، كما المعنيين بمعالجة البيانات الشخصية، في الادارات العامة والخاصة، على المخاطر التي تنطوي عليها هذه العملية، كما عملية انكشافها، وتسربها.

ويمكن البناء في هذا المجال، على التجارب الدولية، أو الإقليمية الناجحة، وعلى التوصيات والاتفاقيات الموجودة، سواء منها تلك التي تعنى بحماية البيانات الشخصية، أو تلك الخاصة ببيانات الاتصالات.

ويبقى الأهم، عدم جواز التعامل مع حماية البيانات الشخصية، من منطلق خطورة اخضاع المستخدمين للرقابة، والتغاضي عن حقهم في معرفة أهداف جمع المعلومات حولهم، وطرق استثمارها، وانكار حق المواطن في المشاركة في عملية اتخاذ القرار، عبر سلب حقه في معرفة كمية المعلومات، التي تجمع حوله، والتي يمكن ان تمنح الآخرين، قوة غير اعتيادية لقيادة حياته والتحكم بها، بحيث تتحول المسألة، إلى مدى قدرة الأجهزة وسيطرتها، والى مدى أحقية تعزيز هذه القدرة، مقارنة مع ما يقره القانون من حقوق وواجبات. ولعل المثل الاوضح، هو امكانية ربط أحد مستخدمي الانترنت، بلائحة الرقابة على الإرهاب، بمجرد استخدامه في البحث على الانترنت، أو في كتابة بريد إلكتروني، عبارات محددة مثل: متفجرات، طائرة، تنظيمات اسلامية، الخ....

الفصل التاسع
التقنيات في التنمية والاقتصاد

١. المعلومات: قيمة اقتصادية

يتفق العارفون والمعنيون، على اهمية تسخير تقنيات المعلومات والاتصالات، في خدمة النمو والتنمية، كما يتفقون على عدم امكانية تجاهل كونها الوسيلة، التي لا يمكن الاستغناء عنها في العديد من النشاطات، واوجه الانتاج المختلفة. الا انهم يتفقون أيضا، على حجم المخاطر التي تواكب استخدامها والاتكال عليها، سواء في المهمات العادية اليومية، أو في المهن والإدارة.

فقد أحدثت تكنولوجيا المعلومات والاتصالات، تحولاً جذريا في جميع أساليب العمل، وممارسة الحياة اليومية، في كافة المجتمعات التي دخلت اليها. وأصبح واضحا للعيان، ان التنمية والنمو، متوقفان بشكل أساسي على توافرها، وحسن استخدامها، وزيادة انتاجها. وقد استثمرت الدول مواردا مالية وبشرية هائلة، لاعداد بنى تحتية، للمعلومات والاتصالات، سعيا منها إلى تطوير خدماتها، وتحقيق التنمية والنمو. الا ان تأثيرها طاول أيضا، المجتمعات التي ما زالت بعيدة عن الافادة من امكاناتها، وعن التمرس بها بشكل أساسي. وقد أنتجت تغيرات هيكلية ونمطية غير متوقعة، على المستويات الاجتماعية، والاقتصادية، والمهنية[295]، والمعرفية، والسياسية والعسكرية، بحيث أصبحت عاملا أساسيا في النمو والانتاج، والتعليم، وممارسة العمل الحكومي، كما في مختلف مجالات التجارة والمال، ما استدعى بروز منظمات محلية، وعالمية، وإقليمية، تعنى بدراسة الافادة من الطاقات الهائلة التي تقدمها، إلى جانب عناية العديد منها، بإدارة المخاطر التي تواكب هذه الطاقات، وبوضع الاطر المناسبة لتأمين الثقة في المجال السيبيري، حيث تنتقل المعلومات، والبيانات، الخاصة بالأفراد، و بالدول، و بروؤس الأموال.

عمليا، تحولت المعلومات إلى قيمة اقتصادية أساسية، كانت وراء إطلاق تسميات، مثل: "عصر المعلومات" و"مجتمع المعلومات" و"اقتصاد المعرفة" وغيرها من مسميات، والتي ان دلت على شيء، فانما تدل على تجذر استخدامها، وتحولها إلى عامل أساس، لا بد من التعامل معه، وضبط انعكاساته، التي لا بد وان تطاول مختلف اوجه النشاط البشري، سواء اكان ذلك سلبا ام ايجابا. فالنشاط البشري، منشئ للحقوق والواجبات، كما انه معلن لها، إلى جانب كونه مصدرا محتملا، للاضرار بالآخرين، وبسلامتهم، وسلامة أموالهم، وامنهم. فاذا كانت شبكات ووسائل الاتصال، مسهلة للانتاج والتبادل وتحقيق الخدمات، الا انها أيضا، أهدافا سهلة للمتخصصين في اختراق الأنظمة. يضاف إلى هؤلاء، الجريمة المنظمة والمجموعات الإرهابية، والناشطون الاجتماعيون، وجيوش الانترنت الوطنية المتخصصة في التجسس، والتي انشئت تحت عنوان: «الجيوش الرقمية[296]»، أو «قوات الدفاع الرقمية».

[295] نشوء نماذج جديدة للأعمال موردي الخدمات، تأجير البرامج الخاصة بالحماية، تيويم البرامج عن بعد
[296] *Iran is building a non-nuclear threat faster than experts ‹would have ever imagined - http://www.businessinsider.com/irans-cyber-army-2015-3 China Reveals Its Cyber war Secrets. http://www.thedailybeast.com/articles/2015/03/18/china-reveals-its-cyber-war-secrets.html*

٢. موجب بناء الثقة

الا ان انتشار استخدام تكنولوجيا المعلومات والاتصالات، على نطاق واسع، وبشكل أساسي، في إدارة البنى التحتية، وتطوير العمل الاداري، خلق بيئة معقدة تكنولوجيا وتنظيميا. في هذا الإطار، كان من الطبيعي ان تطرح تحديات أساسية، امام جميع المعنيين بمجتمع المعلومات وسلامة الفضاء السيبيري، ليس أقلها: حماية البنية التحتية، وحماية البيانات، واعادة تنظيم الادوار والنشاطات، للمستثمرين والعاملين في مجال تكنولوجيا الاتصالات والمعلومات، بحيث تأتي الردود على هذه التحديات، منسجمة مع الانماط الجديدة من النشاط الاقتصادي، ومن توزع الادوار بين القطاعين العام والخاص، ومن المحافظة على القدرة التنافسية، على سبيل المثال. وكما يفترض التعامل مع التقنيات الحديثة قدرة على تذليل الصعوبات التقنية، والتدريب على الممارسات السليمة، فانه يفترض أيضا، إطارا تنظيميا وقانونيا، يضمن الحماية، كما يضمن عدم تحول المخاطر إلى عقبة في وجه التقدم، بحيث لا تتعطل إحدى الخصائص الأساسية لتقنيات المعلومات والاتصالات، اي التبادل، نتيجة لعدم الثقة.

يعتبر الأمن الركيزة الأساسية للمجتمع، بحيث لا يمكن تصور نمو اي نشاط بعيدا عن تحققه، سواء كان على المستوى التقني، ام على المستوى القانوني. وقد تحول الأمن مع مجتمع المعلومات، والحاجة إلى ارساء الثقة فيه، إلى إحدى هذه الخدمات، التي تشكل قيمة مضافة، ودعامة أساسية لانشطة الحكومات، لاسيما في التطبيقات الخاصة بالحكومة الإلكترونية، والصحة الإلكترونية، والتعليم عن بعد. الا ان الوجوه المتعددة للأمن السيبراني، ومضاعفاتها الخطيرة، التي لا تقف عند حدود الاساءة إلى الأفراد، والمؤسسات، بل تتعداها إلى تعريض سلامة الدول والحكومات، تزيد مهمة القيمين على الموضوع، تعقيدا وصعوبة.

في هذا الإطار، يشكل تحقيق الأمن، وارساء الثقة في الفضاء السيبيري، شرطا أساسيا لتسخير تقنيات المعلومات والاتصالات، في مجالات التنمية، خدمة للمجتمعات الإنسانية. ولعل الدليل الحسي على ذلك، ما نجده في الجهود الحثيثة، التي تبذلها الهيئات الدولية، وفي مقدمها الاتحاد الدولي للاتصالات، الذي يؤكد على حتمية الأمن السيبراني، ويخصه بجزء أساسي في برامجه، وخطط عمله المختلفة[297].

وكان الاتحاد قد كلف بالعمل، على بناء الثقة والأمن في مجتمع المعلومات، وذلك عقب القمة العالمية لمجتمع المعلومات. وما ذلك، الا أساس بحثنا، في ضرورة التعاون، ومواكبة المستجدات، بما يتيح لنا العمل الجدي، على تحقيق نمو اقتصادي سليم، وبما يسمح لنا بمواجهة التهديد المتزايد لأمن الفضاء السيبيري، والذي اصبح يجاور، برأي العديدين، تهديد السلام العالمي، لاسيما مع تصاعد الحديث عن الحرب السيبرانية، والإرهاب السيبراني.

[297] الاتحاد الدولي للاتصالات- دليل الأمن السيبراني للبلدان النامية ٢٠٠٧- الموجز التنفيذي – «ولذلك كانت إقامة حلول كافية على صعيد الأمن والثقة تمثل واحداً من التحديات الرئيسية التي يتعين أن يعالجها مكتب تنمية الاتصالات في الاتحاد الدولي للاتصالات في متابعة جهوده لمساعدة البلدان على استعمال الاتصالات وتكنولوجيا المعلومات والاتصالات».

٣. فرص وتحديات

اضحى استخدام تكنولوجيا المعلومات والاتصالات، أحد اهم العناصر في خطط التنمية والاستراتيجيات الوطنية والدولية، في القطاعين العام والخاص، على السواء، حيث تلجا الشركات والمؤسسات كافة، إلى تقنيات المعلومات، في جميع اوجه نشاطاتها، الانتاجية، والتسويقية، والتطويرية أو غيرها. فمع كل صباح، هناك جديد للمعلوماتية والاتصالات، أقله على مستوى اختراق الحواجز، وتقريب الأماكن، وإتاحة الوصول إلى المعلومة. وفي كل ثانية، دفق جديد من المعطيات والمعلومات.

ففي عصرنا الحالي، يعود الفضل الأكبر في تطور الاقتصاد، ونجاح المؤسسات والشركات والمنظمات، لاسيما على مستوى الإدارة، والقدرة على المنافسة، إلى استخدام تكنولوجيا المعلومات والاتصالات. وتقاس قدرتها وامكاناتها، في جزء كبير منها، بمدى قدرتها التقنية، وتطورها.

ولقد أكد قطاع تكنولوجيا المعلومات والاتصالات، على أهميته، من خلال ما أحدثه من تغييرات جذرية في جميع القطاعات الاقتصادية، ومن تحولات في طرق وأساليب العمل، في القطاعات كافة. ولعل اولى بوادر هذا التغيير، ما أفرزه من حاجات جديدة، في البنية التحتية التقنية، وتأمين فرص العمل، وفي إعداد الكادرات البشرية، وتنمية القدرات وبنائها، كما في تأمين البيئة القانونية التمكينية. وكانت القمة العالمية لمجتمع المعلومات، قد شددت على ضرورة استكمال البنية التحتية، كسبيل إلى هدم الهوة الرقمية. ذلك إنها تسمح، بزيادة اتصال الدول بالانترنت، على مستوى اول، وبزيادة اتصال الأفراد، على مستوى ثان.

وهذا يعني عمليا، مزيدا من النشاطات الاقتصادية، سواء عبر بروز خدمات جديدة، أو من خلال الوصول إلى أسواق جديدة، وخفض كلفة الانتاج. وبالفعل، فقد وضع العديد من الدول المتقدمة والنامية، خططا إرشادية، وشارك في خطط إقليمية وبرامج دولية، للتعاون ولتحفيز التنمية، بواسطة استخدام تكنولوجيا المعلومات والاتصالات.

٤. تحديث في التشريع ونماذج العمل

إضافة إلى التحديات التقليدية، التي طرحها دخول تقنيات المعلومات والاتصالات، منذ بداياته، على الآليات التقليدية، للعمل والتحرك، داخل المجتمع، تبرز تحديات جديدة، تستدعي حركة خاصة، يمكن ان تطاول، تحديث نماذج وآليات العمل.

فلتقنية المعلومات والاتصالات، حركة سريعة، ونبض دائم التغيير، وللفضاء السيبراني، سمة عالمية، وطبيعة عالية التقنية، الامر الذي لا يتناسب مع حركة القانون البطيئة، ولا مع الإطار السيادي، الذي يبنى على أساسه. من هنا، لا بد للقانونيين، من الرد على تحديات، ليس أقلها، ربما، إيجاد نماذج تشريعية جديدة، وآليات عمل وهيئات، قادرة على التعامل مع متطلبات السلامة والأمن. وفي القريب العاجل، قواعد جديدة، للتعامل مع مسائل الحوسبة السحابية، والخدمات التي تقدمها شركات خارجية، واجنبية، غريبة عن المؤسسات والادارات، صاحبة الأنظمة المعلوماتية، في القطاعين العام والخاص.

وفي هذا السياق، تطرح مسائل عديدة، منها: اعادة النظر في آليات اصدار التشريع، وإقراره، والهيئات المخولة اقتراح واصدار القوانين والأنظمة، وبرامج اعداد وتأهيل السلطات المعنية بالمكافحة والتحقيق، إضافة إلى استحداث ادارات خاصة، تعالج المواضيع الاجرائية والادارية الخاصة بقطاع المعلومات والاتصالات، ومعالجة المعلومات. ويمكن ايراد بعض الافكار، في هذا المجال، مثل:

- التحول نحو إقرار بعض، القواعد التي تحكم تقنيات الاتصالات والمعلومات، عبر مراسيم عوض عن القوانين، وذلك لكونها، أكثر قرباً من الواقع العملي، ولا تتطلب وقتا طويلا، لوضعها موضع التنفيذ.
- إيجاد هيئات تشريعية منتخبة، ذات صلاحيات مماثلة لصلاحيات المجالس النيابية، تلتزم التشريع في مجال الاتصالات والمعلومات، على ان تراعى التداخلات التي يمكن ان تطرأ، مع القوانين المرعية الإجراء. فالتقنية التي اقتحمت جميع مجالات النشاط الإنساني، تحولت إلى قطاع تجاري، وخدماتي هي الاخرى، ولا بد لتنظيمها والقواعد القانونية الخاصة بها، ان تتاثر بالقطاعات التي دخلتها. ونورد على سبيل المثال، ما يفرض من إجراءات ومواصفات، على البرامج المعلوماتية الخاصة بالاسواق المالية، بحيث تضمن الشفافية، والاطلاع على المعلومات، ومصداقيتها، كما القوة الثبوتية للتقارير الصادرة عنها.
- تشكيل هيئات متخصصة، من المجالس النيابية، تتابع بشكل خاص عمليات التشريع والتنظيم في مجال الأمن السيبراني، ولكن شرط ان تلتزم آلية عمل، تؤمن سرعة إقرار القوانين، وتحديثها، في الوقت المناسب.
- خلق اصول اجرائية خاصة بالتبليغ والانذار، عن الاختراقات وتسرب المعلومات

وفي الوقت عينه، سيكون القضاء مدعوا، للاجابة عن مسائل تقليدية، وتطبيق قواعد كلاسيكية معروفة، على الاوضاع الجديدة، كتحديد صاحب المصلحة في الادعاء في حالات تسرب البيانات، وتقرير ما إذا كان ارتفاع خطر سرقة الهوية، يعطي الشخص حقا في اللجوء إلى القضاء. وما هي امكانية الادعاء على الجهة التي تسربت البيانات من انظمتها، في حال عدم وجود رابطة عقدية، وهل يمكن عندها ان تتم الملاحقة، بسبب التخلف عن اعتماد معايير الحماية الضرورية. كذلك، هل يمكن اعتبار عدم الالتزام بمعايير الحماية، خرقا لقانون حماية المستهلك، ومستخدم الشبكة، إلى ما هنالك من مسائل خاصة بالضرر، الذي يمكن على أساسه المطالبة بتعويض، وكيفية تحديد هذا التعويض.

٥. البيئة المناسبة

لقد تحول الأمن، مع بروز مجتمع المعلومات، والفضاء السيبراني، إلى واحد من قطاع الخدمات، التي تشكل قيمة مضافة، ودعامة أساسية، لانشطة الحكومات والأفراد، على السواء، كما هو الحال، مع التطبيقات الخاصة بالحكومة الإلكترونية، والصحة الإلكترونية، والتعليم عن بعد، والاستعلام، والتجارة الإلكترونية، وغيرها الكثير.

وبالرجوع إلى التعريف الذي يضعه «كتاب الأمن»[298]، لماهية سياسة الأمن[299]، يمكن القول، انه مجموع القواعد التي يضعها مسؤولو الأمن في إدارة النظام، والتي يجب ان يتقيد بها جميع الأشخاص الذين يمكنهم الوصول إليه. وهكذا، يعتبر مفهوم الأمن مفهوما واسعا، يطاول جميع العمليات خلال مراحل الاتصال، وانتقال المعلومات، وتخزينها وحفظها. لذا يمكن القول، انه يشمل، فيما يشمل، أمن الأنظمة الإلكترونية، وأنظمة التشغيل، واستثمار الأنظمة، وأمن الدخول اليها، والى قواعد المعلومات والمواقع، إضافة إلى أمن الاتصالات.

وعلى خط موازٍ، يشمل الأمن، أمن المعلومات، ليس فقط المعنى المادي، اي ضمان عدم تخريبها، أو تشويهها والقضاء عليها، أو سرقتها، بل أيضا، ضمان سريتها، وعدم اطلاع الآخرين عليها، ومصداقيتها، وصحتها.

الا أن الوجوه المتعددة للأمن السيبراني، ومضاعفاتها الخطيرة، تزيد مهمة القيمين على الموضوع تعقيدا وصعوبة، وتستدعي مقاربة شاملة، ومتكاملة، لجميع التحديات التي يطرحها الفضاء السيبراني، بحيث تأتي الردود، والحلول المقترحة، ناجعة وفاعلة. فتحقيقا لأمن، وبناء الثقة في الفضاء السيبراني، من أساسيات تسخير تقنيات المعلومات والاتصالات، في مجالات التنمية خدمة للمجتمعات الإنسانية، على ما جاء في التوصيات الصادرة عن القمة العالمية لمجتمع المعلومات، المنعقدة في تونس عام ٢٠٠٥. في هذا الإطار، اعتبر المنتدى الاقتصادي الدولي، ان المسائل الأساسية على الأجندة الدولية، هي مسائل الاقتصاد الرقمي، مشددا على ضرورة التعاون لمواجهة التهديدات والمخاطر السيبرانية، لتأمين البيئة المناسبة، للافادة من امكانات تكنولوجيا المعلومات والاتصالات في التنمية، ولوضع الإطار الناجع لإدارة المخاطر[300]، وعلى أهمية التركيز على العنصر البشري، لناحية التدريب والتأهيل على الاستخدام الآمن للتقنيات.

٦. العملة الرقمية bitcoins

مع توسع التجارة الإلكترونية، والتبادل الخدماتي عبر الانترنت، وفي رد على حاجات المستهلك، كان لا بد من تطورات تلحق العصب الأساس للتجارة، ولأساليب الممارسة، والايفاء، وغيرها من الامور المتصلة مباشرة بالنشاط التجاري. وكما كانت العملة الورقية، وسيلة معتمدة في التجارة، التي كانت تقوم على الاتصال المباشر، سواء بين التجار أنفسهم، أو بينهم وبين المؤسسات المالية والمصرفية، كان لا بد من ظهور العملة الرقمية، التي تتناسب وطبيعة الاتصالات، التي تتم اليوم عبر الوسائل الرقمية، دون اتصال مباشر مع الزبون.

فالعملة الرقمية، هي البديل عن النقد الورقي أو المعدني، الذي يستخدم في العالم المادي. فباستعمال

[298] *Security handbook, RFC 2196, définit la politique de sécurité comme étant, « une formalisation des règles auxquelles doivent se conformer les gens qui ont accès aux technologies et a l'information d'une organisation ».*
[299] *Securite- Introduction a la securite informatique. www.commentcamarche.net/secu/secuintro.php. La securite des systemes informatiques se cantonne generalemnenta garantir les droits d'accesausdonnees et ressources d'un systeme en mettant en place des mecanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des dites ressources possedent uniquement les droits qui leur ont eteoctroyes.*
[300] *Partnering for Cyber Resilience- Risk and Responsibility in a Hyperconnected World - Principles and Guidelines - http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf*

المال الرقمي، تنتقل الاصول عبر الانترنت، بطريقة رقمية، تمثل النقد الورقي والمعدني. وتحمل العملة الرقمية، أرقاما تسلسلية، تماما كالعملة الورقية أو المعدنية. الا أن النقد الرقمي يختلف عنها، من حيث الجهة التي تتولى اصداره.

ويشير مصطلح العملة الرقمية، أو النقد الرقمي، إلى المال الذي ينتقل إلكترونيا، باستخدام أجهزة الكومبيوتر والاتصالات، لاسيما الانترنت. والمثال الذي يساق في هذا المجال، هو انتقال الأموال[301]، والايداع، وايفاء قيمة الخدمات[302].

وتعمل بعض الأنظمة، تماما كالأنظمة التقليدية، حيث تلجأ إلى ايداع العملة التي تتلقاها من الزبون في مصرف. وتشكل بطاقات الاعتماد، مثالا على التعامل بالعملة الرقمية، حيث تتم تغذية هذه البطاقات، عبر أنظمة مالية إلكترونية. وتطرح هنا، مسألة أمان هذه البطاقات، والتحويلات المالية، التي لا بد وان تجد حماية في القانون، تماما كما هو الوضع بالنسبة للنقد الورقي، وذلك سواء بالنسبة لضمان قيمتها، حيث يتمتع البعض منها بتغطية ذهبية، أو بالنسبة لاثبات الدفع وقيمة السحب، أو الفوائد، أو غير ذلك من الامور، المتصلة بأمان عمليات الايفاء.

وتتنوع عمليات شراء العملة الرقمية، حيث تقوم بعض الأنظمة، ببيع عملتها الرقمية مباشرة إلى المستخدم Paypal and WebMoney، بينما تلجأ أخرى، إلى البيع من خلال طرف ثالث digital currency exchangers. e-gold الا ان تعريف العملة الرقمية يبقى غير مستقر، أو غير دقيق، لاسيما مع التعريفات المتعددة التي اعطيت لها، من قبل منظمات رسمية، G١٠[303] paper.

٧. مخاطر وجرائم

ومع الخدمات المصرفية على الانترنت، يمكن اليوم تحويل الأموال، شراء الأسهم، دفع ثمن المشتريات، وايفاء الفواتير المستحقة، دون أي حاجة لاستخدام العملة الورقية أو المعدنية، أو الشيكات أو غيرها من الاوراق، التي تمثل قيمة مالية ما. وتترافق هذه الخدمات، مع أنواع معينة من الجرائم: كالسطو، والاختلاس، والخداع، والتحويلات الاحتيالية. وتعتبر هذه الممارسات، موازية للجرائم التي رافقت النشاطات المالية والمصرفية التقليدية، والتي كانت تفترض أعمالا مادية، تتناسب وطبيعة المال المادية. فالمبدأ في المنقول، هو أن الحيازة اثبات للملكية. الا أن مخاطر خاصة بطبيعة الانترنت، ترافق استخدام العملة الرقمية هي الأخرى. وتتمثل هذه المخاطر، في الاعطال الإلكترونية، والاعطال على خطوط الاتصال، أو انقطاع الطاقة، أو العثرات التقنية، والاعطال التي يمكن ان تطرأ على الأنظمة المعلوماتية. هذا، بالإضافة إلى المسائل المتعلقة بالخصوصية، وبامكانية تعقب الأشخاص، ورصد حركتهم، وتعريض معلوماتهم الشخصية للانكشاف، وسرقة هويتهم.

[301] *Electronic Funds Transfer (EFT)*
[302] *One rare success has been Hong Kong's Octopus card system, which started as a transit payment system and has grown into a widely used electronic cash system. Another success is Canada's Interac network, which in 2000 at retail (in Canada) surpassed cash [1] as a payment method. Singapore also has an electronic money implementation for its public transportation system (commuter trains, bus, etc), which is very similar to Hong Kong's Octopus card and based on the same type of card (FeliCa). www.Wikipedia.com*
[303] *http://cryptome.org/g10emoney.htm*

وهكذا يمكن لمبيضي الأموال، ان يقوموا بتحويل الأموال المودعة، إلى نقد رقمي؛ بعد اتمامهم لعملية ايداعها، في حسابات عادية لدى المصارف التقليدية، بما يخفي امكانية تتبعها. ويمكن الوصول اليه، من أي جهاز موصول على الانترنت. كما يمكن أن يلجأ المبيض، إلى استخدام التلنيت telenet، بحيث يقوم بالاتصال من خلال جهازه بجهاز آخر، يقع في بلد آخر، يتولى اصدار أمر تحويل الأموال إلى المصرف المعني، بما يساهم في اخفاء الهوية الحقيقية، لمصدر الامر. ذلك أن هذه العملية، تسقط احتمال الربط بين العنوان الإلكتروني للبروتوكول الذي استخدم في عملية النقل، وبين الشخص الذي أصدر الامر. ويؤمن استخدام النقد الرقمي، اخفاء[304] هوية الذي تولى نقل الأموال، سواء بالنسبة للمصرف الذي أصدره، أو بالنسبة للبائع الذي تلقى المبلغ.

كما ان الجمع بين التلينيت والمال النقدي، يزيد صعوبة اقتفاء أثر الشخص، الذي تولى عملية التحويل. كما يمكن لمبيضي الأموال، الاستفادة من امكانات الدفع على الانترنت، ومنها: استخدام بطاقات الاعتماد، سواء بتشفير ارقامها وانتقالها على شبكة مفتوحة، أو عبر التحقق من أرقامها دون استخدام الاتصال المباشر، أو عبر استخدام الشيك الإلكتروني على الانترنت، وتصفية قيمته خارجها. ولا شيء يمنعهم من اللجوء، إلى استعمال البطاقات الذكية، أو البطاقات التي يمكن تعبئة قيمتها stored value card، أو المحفظة الإلكترونية، التي يتم فيها، انتقال العملة الرقمية وتصفيتها على الشبكة في وقت التحويل، وإن كانت هذه الطريقة، لا تستخدم، الا في إيفاء ثمن المشتريات، ذات القيمة المنخفضة والمحدودة.

لذلك، يعتبر توفير الغفلية التامة anonymity، لمستخدم نظام مالي رقمي، حافلا بمخاطر فتح المجال أمام الجريمة الكاملة، أي تلك التي لا يمكن كشفها، لاسيما عندما يمكن تحويل المال، باستخدام هوية شخص آخر، دون السماح بامكانية التعقب. لهذا، كان لا بد من لحظ غفلية مشروطة، بعدم حصول أي جرم، من خلال الحساب العائد للشخص المغفل، حيث يسمح في حال العكس، بالافصاح عن هويته، وبتعقب حركته.

٨. تسهيل تبييض الأموال

يعتبر التزام القاعدة القانونية، والممارسات التجارية المستقيمة، الشفافة، والنزيهة، ضمانا لسلامة النظام الاجتماعي والاقتصادي والاسواق المالية. لذا كان طبيعيا، أن يمتد الاهتمام باخضاع المعاملات الاقتصادية والمالية والتجارية، في الفضاء السيبيري، إلى القاعدة القانونية التي تضمن سلامتها، وسلامة المجتمع، الذي تجري في إطاره، وتمنع تحول التقنيات إلى أداة في خدمة الجريمة، وانتشارها.

من هنا يترافق اللجوء إلى تكنولوجيا المعلومات والاتصالات، في انجاز المعاملات المصرفية والمالية، من تحويل أموال ودفع وفتح اعتمادات، مع تصاعد الاهتمام المحلي والدولي، بإيجاد السبل والآليات، التي تسمح للقانون، ليس فقط بالوجود، وانما أيضا، بالاحتفاظ بفاعليته، في مكافحة الجريمة، بشكل

[304] *ANDRONIKI N. TZIVANAKI- UNIVERSITY OF LEICESTER, ATHENS JANUARY 2001, Information Society services in Southeastern Europe as a means for money laundering. "total anonymity affords criminals the ability to launder money and engage in other illegal activity in ways that circumvent law enforcement." 16 Combined with encryption or steganography17 and anonymous remailers18, electronic cash19 becomes a very powerful medium".*

عام، وجريمة تبييض الأموال، بشكل خاص ، وذلك في مواجهة ازدياد صعوبة كشف هذه الجريمة[305]، عندما تستعين بالتكنولوجيا. اذ تقدم هذه الأخيرة، امكانات لإدارة العديد من الحسابات والخدمات المصرفية، من قبل شخص واحد، من أي مكان في العالم، دون أي اتصال مادي بينه وبين المؤسسة، أو المصرف الذي يوفر له الخدمات.

فالسرية عامل أساسي، في اخفاء أثر الأموال القذرة، وطمس علاقتها بالجريمة. ومن هنا، اعتبار الغفلية على الانترنت، من العناصر التي تشجع مبيضي الأموال، على اللجوء إلى استخدام امكاناتها. والانترنت، تتيح امكانية فتح حسابات، دون انتقال شخصي إلى المصرف، ودون احتكاك مباشر مع المعنيين فيه، إضافة إلى اختيار أسماء وهمية، أو اعتماد مجرد أرقام، للتعريف عن صاحب الحساب. فمع التكنولوجيا، تحولت البنية التحتية المالية، إلى نظام تشغيل دائم الحركة، لا تتوقف فيه حركة انتقال الأموال، لاسيما وان دخول المال القذر، في الاقنية المصرفية العالمية، يجعل تعقبه، ورصد حركته، أكثر صعوبة.

وكانت الFATF، قد أشارت إلى هذا الواقع، في أحد التقارير الصادر عن خبراء لديها، في موضوع الخدمات المصرفية الإلكترونية، حيث اعتبرت أن هذه الأخيرة، تشكل وسيلة جديدة، تسهل عمل مبيضي الأموال، اذ تساعدهم على اخفاء هويتهم، ما يرفع مستوى السرية، التي تضمن هامشا أكبر من الأمان، لدى تنفيذ مراحل التبييض المختلفة.

ويدخل تبييض الأموال، في دائرة الجريمة المنظمة ، التي تستخدم الفضاء السيبيري، كمصدر جديد للعائدات والأموال[306]، والتي استطاعت الافادة من تكنولوجيا المعلومات والاتصالات، عبر الجمع بين امكانات الوسائل الإلكترونية، والوسائل التقليدية، بحيث ازدادت صعوبة كشف مصدر الأموال القذرة، وتتبع حركتها. فالجريمة المنظمة، بحاجة إلى اخفاء المصادر القذرة لعائداتها، بغية محو الأثر الذي يربطها بالجريمة، التي نتجت عنها. لذا فإنها تلجأ إلى تبييضها، عبر سلسلة من الأعمال، التي تهدف إلى ادخال المال في الدورة الاقتصادية، بما يضفي عليه الصفة الشرعية، ويعطيه مصدرا نظيفا، لا يثير الشبهات حول الأشخاص الذين يتعاملون به. ومن هنا، تعتبر مكافحة تبييض الأموال، جزءا من مكافحة الجريمة المنظمة[307]. وغني عن القول، ان الموظفين الرسميين، كما المسؤولين السياسيين الفاسدين، بحاجة إلى تبييض أموال الرشوة، والأموال المختلسة من الخزينة، ومن المساعدات الدولية، التي تخصص لدعم النمو في بلادهم.

يشكل البرنامج العالمي لمكافحة تبييض الأموال[308]، العنصر الأساس، الذي يستخدمه جهاز مكافحة الجريمة والمخدرات. فمن خلال هذا البرنامج، تمكنت الأمم المتحدة من مساعدة الدول المختلفة، على ادخال تشريعات لمكافحة تبييض الأموال، وعلى دعم وتطوير آليات مكافحة هذه الجريمة، عبر تشجيع

[305] *The Ten Fundamental Laws of Money Laundering, "The greater the facility of using cheques, credit cards and other non-cash instruments for effecting illegal financial transactions, the more difficult it is to detect money laundering".United Nations office on Drug and crime.*
[306] *With the growing amount of financial data stored and transmitted online, the ease of computer intrusions add to the severity of traditional crimes such as identity theft; to putthis in perspective for the digital ageover USD$222 billion in losses were sustained to the global economy as a result of identity theft. Of this $222B most was laundered online through various e-channels. http://cybrinth.com/uploads/Money%20Laundering%20in%20Cyberspace.pdf*
[307] الأموال القذرة تستخدم فقط بطريقة مباشرة، في تمويل الأعمال الإرهابية
[308] *Global Programme against Money Laundering (GPML)*

تطوير سياسات مكافحة التبييض، وتقديم المساعدة التقنية، واعداد الدورات التدريبية، ونقل الخبرات إلى العاملين في المؤسسات المالية، والهيئات القضائية، والأمنية، والاشراف على دراسة الموضوع، وتحليله، والتوعية حول خطورة هذه الجريمة.

وقد أوردت التوصية الأوروبية، لمكافحة تبييض الأموال، في هذا السياق، أن مكافحة تبييض الأموال، هي من الوسائل الأكثر فاعلية في التصدي للجريمة المنظمة[309]، وفي مقدمها: الاتجار غير المشروع بالمخدرات والمؤثرات العقلية، والدعارة، والفساد.

أ- التبييض وتهديد الاقتصاد

ولتبييض الأموال أثر سيئ على الأعمال، كما على النمو، وعلى الاقتصاد، ودور أكيد في دعم الجريمة المنظمة والفساد، كونه يرفدها بالإمكانات المالية الضرورية، لتجنيد المزيد من المجرمين والفاسدين. ويؤدي التغاضي عن تبييض الأموال، إلى تآكل الاقتصاد، في البلد الذي يمارس فيه، وذلك عبر التغيرات التي يدخلها على حركة النقد، وقيمة الفوائد والتضخم، ومن ثم عبر تبخر ملايين الدولارات سنويا، بعد استثمارها في الدورة الاقتصادية الشرعية. وفي هذا التأثير السلبي على الاقتصاد المحلي، تأثير لا بد أن يستشعره الاقتصاد العالمي.

أما البلدان التي تتساهل مع ضخ أموال قذرة في اقتصادها، كعامل مساعد على الانماء، فانها ولا شك، ستجد صعوبة كبيرة في استقطاب عمليات الاستثمار، على المدى الطويل، والثابت، من قبل المؤسسات، والهيئات النظيفة السمعة. فهذه الأخيرة تبحث عن الاستقرار، والإدارة الجيدة، وحكم القانون، أي عن العوامل التي تساعدها على دعم التطور، والنمو المستمر، على المدى الطويل. وأهم شروط هذه الجريمة هي السرية.

والقاعدة أن رؤوس الأموال الباحثة عن الشرعية، لا تَبْني اقتصادا، ولا تحقق تنمية اقتصادية حقيقية، حيث لا يهتم غاسلو الأموال بالجدوى الاقتصادية للاستثمار، قدر اهتمامهم بالتوظيف، الذي يسمح بتبييض تلك الأموال. ولعل الأخطر من هذا كله، هو العلاقة بين تبييض الأموال والإرهاب[310]. ففي كلمة لرئيس مجموعة العمل المالية، Groupe d'Action Financière، التي ألقاها في باريس، بتاريخ ٢٩ حزيران ٢٠٠٧، حول تقرير مفصل أعدته نتيجة دراسة عن وسائل تبييض الأموال، في قطاع العقارات، إشارة واضحة، إلى استخدام نماذج متشابهة، من عمليات الاستثمار والتمويل ، في تبييض الأموال وفي تمويل الانشطة الإرهابية[311]. الامر الذي يشير الى، ضرورة اضطلاع الدول، بمسؤولية السهر على عدم تحويل الطرقات السريعة للمعلومات، إلى طرق سريعة وآمنة لتبييض الأموال، لما بين هذه الجريمة، والجرائم الخطيرة الأخرى، من ترابط وثيق، جعل الدول تتعاون على مكافحتها، منذ ما قبل بروز الفضاء السيبيري.

[309] في مقدمة التوصية الأوروبية لمكافحة تبييض الأموال
Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering. Moreover, the preamble of the above mentioned EC Directive acknowledges: "combating money laundering is one of the most effective means of opposing [organized crime in general and drug trafficking in particular]".

[310] كتاب تبييض الأموال والإرهاب: تعقب الجريمة عبر القنوات المالية- منشورات ايدريل بيروت ٢٠٠٤ د. منى الاشقر ود. محمود جبور

[311] *M. Frank Swedlove, Président du Groupe d'action financière. Résumé du Président, Paris, réunion plénière, 27 au 29 juin 2007, 29 Juin 2007, « Le rapport sur le blanchiment de capitaux et le financement du terrorisme dans le secteur immobilier étudie les vulnérabilités de ce secteur au regard du blanchiment de capitaux et du financement du terrorisme. Il s'agit du premier rapport approfondi du GAFI sur cette question. Il identifie les méthodes les plus courantes de blanchiment de capitaux associées aux opérations, aux investissements et au financement dans le secteur immobilier. Ce projet démontre que ces mêmes méthodes ont été utilisées dans des schémas financiers potentiellement liés à des activités terroristes ».*

ب- وسائل جديدة وردود ملائمة

وتتشابه طبيعة جريمة تبييض الأموال، وطبيعة الجريمة السيبيرية، من حيث عبورها الحدود، وظهور آثارها في مكان، غير ذلك الذي وقعت فيه الجريمة، التي أنتجت الأموال. وعلى غرار الفضاء السيبيري، تشكل هذه الجريمة، تحديا ديناميكيا، للقانون وآليات تطبيقه. وذلك، نظرا للتحولات المستمرة التي تطرأ على وسائل وأساليب التبييض، المعتمدة من قبل المجرمين، ما يعني تغييرا وتطورا مستمرين، لوسائل وأساليب المكافحة.

فمن المتعارف عليه، انه لا بد لأسلوب مواجهة أي جريمة، من أن يواكب أسلوب ارتكابها. ولا ينفك الجناة في جرائم تبييض الأموال، يستنبطون وسائل وأساليب جديدة، في ارتكاب جرائمهم، فكان أن لجأوا مؤخرا، إلى امكانات الوسائط الإلكترونية، واهمها استعمال الكومبيوتر، وشبكة الإنترنت، وبرامج الاختراق للحسابات المصرفية، وذلك للتلاعب بها، ونقلها، وتحويلها عن بعد.

لذا، يبدو من الضروري، أن تستعمل المؤسسات المصرفية، الأنظمة المضادة لهذا الاختراق، وان تراقب حركة الحسابات إلكترونياً، سواء في ذلك، حركات السحب، أو الإيداع، أو التحويل، أو النقل من الداخل إلى الخارج، أو العكس. كما يبدو ضروريا أيضا، لجوء أجهزة المكافحة والأمن، إلى الوسائل الإلكترونية، هي الأخرى، سواء منها الأجهزة أو البرامج.

فتبييض الأموال، كما الفضاء السيبيري، ظاهرة عالمية، تطاول تقريبا المجتمعات كافة، ما يستدعي متابعة ومعالجة، تتضافر فيهما جهود البلدان المختلفة، لانجاح تدابير المكافحة.

ج- مراحل التبييض

تعرف الاتفاقية الأوروبية تبييض الأموال بانه: كل تحويل أو نقل لملكية، مع العلم المسبق، أن هذه الملكية ناتجة عن نشاط جرمي، أو عن مشاركة فيه، وذلك بغرض اخفاء أو تمويه المصدر غير الشرعي للملكية، أو بغرض مساعدة أي شخص متورط في ارتكاب نشاط مماثل، للتملص من النتائج القانونية لهكذا عمل. وعليه، فتبييض الأموال هو امتلاك، وحيازة، أو استعمال الأموال، مع معرفة مصدرها الجرمي، عند وقت تلقي الملكية.

ولا تختلف مراحل جريمة تبييض الأموال، عند استخدام الوسائل الإلكترونية، عنها في الوسائل التقليدية، بل تبقى هي نفسها، أي الايداع، والتكديس، واعادة ضخ الأموال في الدورة الاقتصادية الشرعية.

ويعتبر الايداع، المرحلة الأولى والاصعب، لانها الاشد خطورة لناحية احتمالات كشف المجرمين فيها. أما المرحلة الثانية، فهي المرحلة التي تتم خلالها تغطية مصدر المال، بحيث يصعب على السلطات المعنية كشفه، في حال حاولت الاستقصاء والبحث. أما اعادة ضخ المال، فهي المرحلة، التي تضفي الصورة الشرعية الظاهرية، على هذا المال.

وتسمح تكنولوجيا المعلومات والاتصالات، بتحريك المال القذر، في جميع مراحل التبييض، بدءا من مرحلة الايداع، مرورا بتوظيف هذا المال في مشاريع وهمية، يعلن عنها على الانترنت، وتخصص لها المواقع، وتحدد أساليب وشروط الاكتتاب، وصولا إلى الاستثمار بعد ذلك، في مشاريع قانونية، والدخول في الدورة الاقتصادية.

فعلى الانترنت مثلا، يمكن فتح حسابات إلكترونية، إلى جانب الحسابات العادية، وتحريك الأموال المودعة فيها جميعا، عن بعد، وفي وقت واحد.

ومع الخدمات المصرفية الإلكترونية، التي تقدمها معظم المصارف، يمكن القيام بعمليات معقدة، ينتقل بها المال عن بعد، من حساب إلى آخر، ومن مصرف إلى آخر، ومن قارة إلى قارة اخرى، إلكترونيا، وتلقائيا، بحسب توقيت يحدد بشكل مسبق، يبرمج بطريقة أوتوماتيكية، ولا يستدعي أي تدخل، كالانتقال الشخصي إلى المصرف، والتوقيع من قبل صاحب الحساب.

د- آليات التبييض

يفترض الاسلوب التقليدي في تبييض الأموال، بذل جهود مادية، مثل نقل الأموال، وجمعها، والانتقال إلى المصرف لايداعها. وذلك باعتماد أساليب تمويهية، والحرص على عدم لفت انتباه السلطات المعنية بمراقبة الدخل، بما يمكن أن يثير التساؤل والشبهات، حول مصدر الأموال المودعة. لذا غالبا ما لجأ المبيضون إلى ارسال الأموال النقدية، إلى مصارف خارج البلاد، التي وقعت فيها الجريمة، وتحديدا، باتجاه بلاد ذات أنظمة رقابة متساهلة، أو باتجاه البلاد التي تعتبر بمثابة الجنات الضريبية. هذا عدا عن أعمال الرشوة، وعمليات شراء العقارات، والأموال العينية الاخرى.

وكان المبيضون قد حرموا، من امكانية ايداع مبالغ تتجاوز حدا معينا من المال، بعد إقرار قوانين لمكافحة تبييض الأموال، تنص، فيما تنص، على ضرورة تقديم تصريحات خاصة، حول مصدر الأموال، والنشاط الذي يقومون به. وقد اضطرهم هذا الامر، إلى إجراء عمليات ايداع متعددة، واستخدام عدد من العملاء لاتمام هذه العمليات، مع ما يعنيه ذلك، من ضرورة الانتقال، من مصرف إلى آخر، أو من فرع إلى آخر.

أما اليوم، فقد سمحت لهم تكنولوجيا المعلومات والاتصالات، بتجاوز هذا الحرمان، عندما أزالت العوائق المادية، التي كانت مفروضة على انتقال الأموال، بدءا من جمعها، مرورا بنقلها، وصولا إلى ايداعها، مضيفة إليها تقنيات التشفير، التي تساعدهم على إجراء عملياتهم المالية، بسرية تكاد تكون تامة. اذ يمكن أن تنتقل الأموال عبر الانترنت، من بلد إلى آخر، ومن مصرف إلى آخر، ومن عملة إلى أخرى، دون أي حاجز أو مانع مادي، يعرض ناقلها إلى الانكشاف، أو يعرضها للضياع وللتلف.

كذلك، تفتح الانترنت مجالات واسعة للاستثمارات، بدءا من الاستثمار في ملكية الشبكات، مرورا بالاستثمار في شراء الأجهزة والبرامج، وصولا إلى إنشاء الشركات والمؤسسات التجارية، التي تقدم الخدمات، وتجري الصفقات التجارية. من هنا، لا بد من تنظيم الأعمال التجارية، ليس فقط انطلاقا من ضرورة حماية الاستثمارات، وتأمين عامل الثقة، بل أيضا، من الحاجة إلى منع استثمار جزء من النشاط

التجاري، في خدمة الجرائم الاقتصادية، لاسيما منها، تلك التي ترتبط بالإرهاب، وبتجارة المواد الممنوعة، كالمخدرات، والمؤثرات العقلية. فالتحويلات المالية الرقمية، digital transactions، تصبح أكثر سهولة في النقد الرقمي digital cash، وأكثر قدرة على خدمة تبييض الأموال، في التحويلات التي تتم دون تحديد لهوية الأشخاص أصحاب النقد، ذلك إنها لا تترك أثرا في سجلات، يمكن اعتمادها في الملاحقة، وتتبع أثر المجرمين.

هـ- هيئات المكافحة

نتيجة لما تقدم، كان طبيعيا أن تبادر الدول الحريصة على مكافحة جريمة تبييض الأموال، إلى تأمين مواكبة أكثر ملائمة لحركة الأموال، على مستوى التشريع، والتعاون القانوني الدولي. وبالفعل، فقد انشئت العديد من الهيئات المتخصصة، الإقليمية والدولية، في مختلف قارات العالم، وحشدت الدول جهودها، لتحقيق نجاح هذه المكافحة، وان بالحد الممكن[312].

وقد أدى هذا الأمر، إلى بروز عدة هيئات على الساحة الدولية، تتعاون فيما بينها، لمكافحة جرائم مكافحة تبييض الأموال. ففي عام ١٩٩٢، تم توقيع اتفاقية ماستراخت، التي نصت على إنشاء هيئة الايروبل Europol، وهي هيئة معلومات بدا نشاطها عام ١٩٩٤، لمكافحة الاتجار بالمخدرات والجريمة المنظمة. وفي العام ١٩٩٥، وقعت إتفاقية الايروبل، بهدف تأكيد التعاون الدولي في مكافحة الاشكال الخطيرة للإجرام الدولي: ومنها جرائم تبييض الأموال. وفي فرنسا، انشئت هيئة تراكفين Tracfin بموجب القانون الصادر في ١٢ يوليو ١٩٩٠ ، وهي إحدى هيئات وزارة الاقتصاد والمالية، وتختص بتلقي المعلومات من المؤسسات المالية ، لتقوم من ثم بتحليلها واستخلاص النتائج، فيما يتعلق بجرائم تبييض الأموال. وفي بريطانيا العظمى، تم إنشاء وحده مالية تختص بتتبع تبييض الأموال، ذات المصدر غير المشروع، وتهريب المخدرات، أطلق عليها، اسم NCIS، وهي إدارة وتحليل معلومات،حول عمليات مشتبه فيها، تم ضبطها من قبل الشرطة المعنية.

كما أنشئت في البرتغال، على غرار هذه الهيئات، هيئة DCCCFIEF[313] وهي الإدارة المركزية لمكافحة الفساد، والتحايل، والجرائم الاقتصادية والمالية، وفي بلجيكا هيئة CTIF، والتي انشئت عام ١٩٩٣، وهي وحدة لمعالجة المعلومات المالية. وفي هولندا هيئة MOT عام ١٩٩٣. وفي مصر وحدة مكافحة تبييض الأموال عام ٢٠٠٢. وقد أكدت اتفاقية المجلس الأوروبي، التي صدرت في ستراسبورج، عام ١٩٩٥، على حق الدول الأعضاء في الاتفاقية، ان تطلب من بعضها البعض، المعلومات اللازمة، التي تساعدها في كشف جرائم تبييض الأموال، الناتجة عن جرائم وقعت على الاقليم، الخاضع لسيادتها.

و- دور القطاع المصرفي

تحتاج المصارف إلى المصداقية والسمعة الحسنة، كي تحوز ثقة المتعاملين معها، لا بل أن نجاحها يقوم، إلى حد كبير، على مدى توافر هذا العنصر لديها، كونها تتعامل بأموال الغير. ومن هنا أهمية تنبهها إلى

[312] *The United Nations, the Bank for International Settlements, the OECD›s FATF (Financial Action Task Force), the EU, the Council of Europe, the Organisation of American States, all published anti-money laundering standards. Regional groupings were formed (or are being established) in the Caribbean, Asia, Europe, southern Africa, western Africa, and Latin America.*
[313] *Directorate for the fight Against Corruption, Fraud, and Economic and Financial Infringements. Portugal. http://www.palgrave.com/PDFs/0333802985.PdfJames L. Newell and Martin J. Bull*

سمعتها، التي لن تبقى سليمة، مع انخراطها في عمليات تبييض الأموال. فالمؤسسات المالية المحترمة والكبيرة، لن تتعامل مع مؤسسات مالية ذات سمعة سيئة، والمصارف ذات السمعة الجيدة ستهتز، لو تعاملت مع المجرمين. وستحجم كبريات المؤسسات الاقتصادية، حتى المتورطة منها، على التعامل معها، خوفا على سمعتها هي الأخرى، وعلى صورة أموالها، ونظافة مصدرها.

ويشكل استثمار المصارف لأموال الودائع لديها، تغطية مناسبة، ومرحلة هامة لتبييض الأموال، كونها تخلط الأموال القذرة، بالأموال النظيفة أولا، وتؤدي الفوائد إلى أصحاب رؤوس الأموال المستثمرة، ثانيا. وتشكل القروض بضمان الودائع، أحد أوجه تبييض الأموال، مع الفرصة التي توفرها لاستثمار القرض، في مشاريع قانونية. كما أصبح الاستعمال الشائع للبطاقات الممغنطة، أمرا مساعدا لإخفاء مصدر المال، دون الاستعانة المادية المباشرة، بالمصرف الذي أودع المال فيه، حيث يمكن ان يتم سحب الأموال، عن بعد، ومن دولة أخرى، غير تلك التي تمت فيها عملية الايداع. لذا، تجري عمليات تبييض الأموال، في القطاع المصرفي، والخدمات المالية، بشكل أساسي، بتوزيع ونشر كميات ضخمة من الأموال، عبر عدد من الحسابات.

ولذا كان من الطبيعي، أن تحاول الجهات المعنية بمكافحة هذه الجريمة، وضع سياسات لضبط حركة الأموال، التي تتداول على هذا المستوى.

ويندرج في هذا الإطار، التغيرات التي طرأت، والتي حولت المصارف إلى هيئات مكافحة، يطلب منها، مراقبة العمليات التي تتم بواسطتها، ونوعيتها. كما يفرض عليها، الالتزام بالتوصيات والتعليمات الخاصة بالتعرف إلى هوية الزبون، ونوعية نشاطه، والتحقق من شرعية مصدر أمواله، وان بالحد الأدنى.

وكانت التوصية الصادرة عن اللجنة الأوروبية، قد اعتبرت تحديد هوية الزبون، ضروريا في كل تحويل تبلغ قيمته ١٥٠٠٠ يورو، أو أكثر، سواء أجري التحويل في عملية واحدة، أو من خلال عدة عمليات تبدو متصلة[314]. كذلك تولت الFATF[315]، تقديم عدد من الاقتراحات، في إطار تفعيل مكافحة التبييض في الفضاء السيبراني، تناولت: تشديد الإجراءات حول التعريف بهوية الزبون، تطوير الإمكانات على مستوى تكنولوجيا المعلومات، لرصد التحويلات المشبوهة، والتحقق من هوية الزبون، إضافة إلى منع المؤسسات المالية، من تقديم خدماتها على الانترنت، ما لم تكن حائزة على الترخيص القانوني، من السلطات المختصة، في مكان ممارستها لنشاطها هذا[316].

هذا، وكانت ال[317] FATF ، قد أشارت منذ العام ٢٠٠١، في التقرير الذي أعدته، إلى خطورة تحول العاب القمار على الانترنت، إلى جنة لعمليات تبييض الأموال[318].

الا أن هذه الجهود، لم تثبت حتى اليوم، فاعلية ترتقي إلى مستوى الجريمة، وانتشارها، وآثارها السلبية، وذلك باعتراف المختصين والمسؤولين عن مكافحتها، نظرا للصعوبات العملية، وتضخم المعلومات

---

[314] *Article 3(2) of the EC Directive, identification is required “for any transaction (...) involving a sum amounting to 15.000 Euro or more, whether the transaction is carried out in a single operation or in several operations which seem to be linked”.*
[315] *75 FATF-XI, 2000, n 14 above, p.4. In Androniki N. Tzivanaki Information society services in South Eastern Europe as a means for money laundering*
[316] *This measure is also considered in the framework of an ANNEX to be included to the EC antimony laundering Directive, which is currently under amendment [Directive 91/308/EEC, n 5].*
[317] *Financial Action Task Force on Money Laundering*
[318] *Rapport annuel 200-2001, http://www.fatf-gafi.org/dataoecd/42/22/35394319.pdf*

والتقارير التي تقدم. ويمكن تقديم مثال على ذلك، اهمال تقرير أحد المصارف، الذي قدم، نتيجة الاشتباه بتحويل تم إلى أحد حسابات المجرمين، الذين نفذوا اعتداءات الحادي عشر من ايلول[319]. هذا مع الإشارة، إلى مبادرة العديد من الدول، نتيجة لهذه الاحداث الأخيرة، إلى تشديد الإجراءات الخاصة بتبييض الأموال، سواء عبر نصوص جديدة، أو عبر تعديل ما كان معمولا به. كذلك ما زالت مواجهة تبييض الأموال، باستخدام تكنولوجيا المعلومات والاتصالات، غير كافية في العديد من البلدان، لاسيما منها العربية، ذلك أن تبييض الأموال، بالوسائل المعلوماتية وباستخدام الفضاء السيبراني، يعد من الجرائم الاقتصادية الحديثة نسبيا، هذا عدا عن النقص الأساسي، على مستوى مكافحة جرائم المعلوماتية، والجريمة السيبيرية، في هذه البلدان.

ز- البيانات الشخصية في الملاحقة

تعتبر سهولة الاتصال، بين مقدمي الخدمات والزبائن، من العناصر الأساسية في الاقتصاد الجديد، أو اقتصاد المعرفة، واقتصاد المعلومات. الا أن الزبائن، لا يبدون حماسة، في اعطاء البيانات والمعلومات الشخصية، في كل مرة يطلب منهم ذلك، مقابل ما يشترونه من بضاعة أو خدمات. ويلاحظ في هذا المجال، ميل لدى العديد من مستخدمي الانترنت، إلى استعمال أسماء مستعارة، أو تقديم معلومات مغلوطة، لدى اضطرارهم إلى تعبئة استمارة، تحتوي معلومات شخصية، سواء لاعطائهم حق الدخول إلى موقع، أو الافادة من خدمة معينة، تستدعي التأكد من بعض الامور الشخصية. وينطلق هذا الميل، من أن الانترنت والفضاء السيبراني، مساحة يفترض أن تكون حرة للحركة، بعيدا عن التحريات. وإذا كان كثر متمسكين بحقهم في الحفاظ على خصوصيتهم، في العالم الحقيقي، فهم غير مستعدين للتخلي عنها، في الفضاء السيبراني.

في هذا السياق، تطرح إشكالية الحق في الخصوصية، والذي تدعمه ممارسات الغفلية، في التحويلات والنشاطات التجارية على الانترنت، من جهة، وفي استخدام البرامج المتخصصة، في كشف نماذج هذه النشاطات، التي يمكن أن تشكل تبييض أموال، من قبل الأجهزة الأمنية المتخصصة، من جهة أخرى.

فقد طورت الشركات التجارية، العديد من البرامج، التي ترتكز إلى تقنية التنقيب في البيانات Data Mining، والتي تهدف، بشكل أساسي، إلى معالجة ملايين البيانات، تحقيقا لغايتين: الوصف description، والتوقع Prediction[320]. ومع استخدام هذه التقنية، يمكن للسلطة التي تتولى مكافحة التبييض، تحديد مواصفات العمليات، وتحديد أطياف للأشخاص، الذين يمكن أن يقوموا بنشاط تبييض الأموال، وتعقب حركتهم تبعا لذلك، في ملايين الملايين من البيانات الشخصية والمهنية، المخزنة لدى موفري خدمات الانترنت، والمؤسسات المالية والتجارية المختلفة.

---

[319] *One bank actually reported a suspicious transaction in the account of one of the September 11 hijackers - only to be ignored.*

[320] أعمال مؤتمر: «معالجة المعلومات القانونية في القرن الحادي والعشرين وتحدياتها»، بيروت ٢٠٠١- منشورات صادر ص: ٢٢٧

- Mining Data Warehouses to Improve Decision-Making Process, Dr. Aziz Barbar, "from a general point of vew, the two main goals of Data Mining are description and prediction. FAYY96 gives a more precise definition: knowledge discovery in databases is the non-trivial process of identifying valid, novel, potentially useful and ultimately understandable patterns of data."

ح- الإطار القانوني

تركز النصوص القانونية حول مكافحة تبييض الأموال، على الدور الايجابي، الذي يمكن أن يلعبه القطاع المالي والمصرفي، في الحد من امكانات توسع هذه الجريمة، لاسيما وأنه المعني الأول، بنتائجها وآثارها السلبية. لذا، تشدد القواعد القانونية، في البلدان المعنية، على التزامات المؤسسات المالية والمصرفية، كما على التزامات أندية القمار والمؤسسات العقارية، في الابلاغ، والاحتراز، وتطبيق الإجراءات الادارية، والقانونية، التي تساعد على تحديد هوية الزبون، وحركة الأموال، لدى اتمام العمليات والصفقات، التي تبلغ أو تتجاوز قيمة مالية معينة.

وترتكز هذه السياسة، بشكل أساسي، على مفهوم الصلاحية المكانية، بمعنى افتراض حصول التحويلات والعمليات المالية، ووجود الأفراد والمؤسسات في الإقليم الخاضع لسيادة الدولة المعنية بقانون المكافحة. وإذا كانت هناك احتمالات، لعدم تواجد الزبون في الإقليم نفسه، الذي تتواجد فيه المؤسسة، الا أنه عادة ما يطلب اليه، تحديد مكان اقامة مختار، حيث تمارس المؤسسة نشاطها المسجل، والمرخص قانونا. لكن الوضع مع الانترنت يختلف، فالتحويل يمكن ان يحصل، في مكان وجود خادم server الشركة، من خلال موقعها الإلكتروني، أو مركزها الأساسي، أو حتى على جهاز العميل أو الزبون، حسب القانون، أو التقنية المستخدمة.

كذلك تتيح الانترنت لهذه المؤسسات، العمل دون الاستحصال على اي اذن رسمي، من خلال المواقع التي تنشئها، ما يجعلها خارج دائرة الالتزامات المفروضة، على تلك التي تخضع لهذا الاذن في العالم المادي، ما يزيد صعوبة الرقابة على عمليات تبييض الأموال، التي يمكن أن تحصل من خلالها.

فمزود خدمة الانترنت، الذي يحفظ البيانات الشخصية الخاصة بزبائنه، لا يملك سببا يدفعه للشك في نشاط هؤلاء، سواء أكانوا يعملون بصورة مغفلة تامة، أم نسبية. كما لا يمكن الطلب من هذا المزود رصد، وتعقب حركة زبائنه، لكشف حقيقة نشاطهم، لاسيما وان في هذا التصرف من قبله، مخالفة قانونية واضحة، لطبيعة المهمات التي يتولاها، بصفته القانونية، والتي يمكن توقعها منه. كما أن فيه تعرضا لحق الزبائن في العمل بحرية، وفي الحفاظ على خصوصيتهم. ولا تخرج المصارف، أو مقدمو الخدمات المالية، عن هذه القاعدة، عندما ينشط المبيضون، من خلال الخدمات التي يتيحونها.

فالدور الأساسي هنا، يعود إلى المؤسسات والسلطات الرسمية، التي تفرض القاعدة القانونية، بما يتناسب وطبيعة النشاط، وامكانات التطبيق، على المؤسسات المالية والمصرفية، المنشأة والعاملة، حسب الاصول القانونية المرعية الإجراء.

على خط مواز، يسمح بعض أصحاب أندية القمار على الانترنت لزبائنهم، بإنشاء المحفظة الإلكترونية، وفتح الحسابات، مقابل بيانات شخصية، لا توازي تلك التي تقدم إلى المؤسسات المالية، في العالم المادي. ويمكن لهؤلاء أن يكونوا، أحيانا كثيرة، على علم بنشاط زبائنهم المشبوه، فيغضون الطرف عنه، لما يمكن أن يعني لهم من أرباح. فالتبييض بهذه الطريقة، يفترض ربح الأموال من قبل الشخص، الذي يمارس القمار، الأمر الذي لا يعتبر حاصلا بالضرورة. وبالتالي يكون مزود الخدمة، هو الذي يستفيد من العملية. يضاف إلى ذلك، أن رصد الزبون المشبوه، أو إعلان مسؤوليته عند التأكد من

نشاطه، يبقى غير مضمون، مع غياب إمكانية تحديد هويته، من خلال البيانات الشخصية المغلوطة، التي يكون فد صرح عنها، لدى الاكتتاب.

ويزداد الامر خطورة، مع الإمكانات التي تقدمها الشركات المتعددة الجنسيات، على مستوى تحويل الأموال، والخدمات المصرفية على الانترنت، حيث تتفاقم صعوبة الكشف عن هوية أصحاب التحويلات والحسابات، لاسيما منها، تلك التي تستخدم فيها أسماء وهمية، أو معلومات رقمية.

كذلك يشكل دخول الاتصالات الخلوية، على خط هذه الخدمات، تعقيدات اضافية، تمنع التعرف إلى محركي الحسابات والمودعين. ويضاف إلى ذلك، السرية التي تحيط بهوية المشاركين في ألعاب القمار على الانترنت، كما في المزايدات، والصفقات التجارية العقارية، وغيرها.

وتتفاقم صعوبات كشف الهوية، وكشف عمليات تبييض الأموال، مع انضمام استخدام العملة الرقمية، في ألعاب الميسر، وفي فتح الحسابات والاعتمادات المصرفية، ومع غياب التشريعات الملائمة، ، ما جعل المعنيين بمكافحة هذه الجريمة، ينكبون على اجراء دراسة خاصة، حول المخاطر التي تمثلها هذه الآليات، كوسيلة يمكن استخدامها من قبل أصحاب رؤوس الأموال القذرة، لتنفيذ جرائم التبييض[321]. وبالرغم من منع هذه الالعاب، بواسطة الاتصال المباشر(online)، في تشرين الثاني (أكتوبر) من العام ٢٠٠٦، من قبل الولايات المتحدة الأميركية، ما زالت السيطرة على هذه الالعاب، بواسطة الهاتف الخليوي، مستبعدة، نظرا لغياب التشريع الخاص، الذي يمكن تطبيقه، على المقامرة بهذه الطريقة. ويتضح حجم الخطر الذي تمثله هذه الالعاب، نظرا للعدد الكبير لمستخدمي الانترنت، الذين يكتتبون فيها[322].

ط- القرصنة والاعتداء على الملكية الفكرية

كما تؤثر الجريمة السيبرانية بشكل أساسي على الاقتصاد، من زاوية الاعتداء على حقوق الملكية الفكرية، عبر عملية القرصنة، التي تروج للاستخدام أو للنسخ، لبرامج وتطبيقات معلوماتية، ومواد أخرى كالافلام والموسيقى، الخاضعة لحقوق الملكية الفكرية. وتساهم العديد من المواقع على الانترنت، في الترويج لبرامج مقرصنة مجانا، أو بمقابل مادي ويمكن للقرصنة، استهداف أجهزة بغاية تدميرها، أو تحقيق مكاسب مالية شخصية، عندما يلجأ مقتحم النظام، إلى سرقة معلومات بطاقات الائتمان، وتحويل الأموال من حسابات مصرفية مختلفة، إلى حساب المقرصن الخاص، أو أي حسابات أخرى.

على مستوى آخر، يعتمد بعض المقرصنين، على ابتزاز الشركات العالمية، وتهديدها بنشر المعلومات السرية الخاصة بها، في حال عدم قيامهما بدفع، أو تحويل المبلغ المالي المطلوب.

[321] *UMultinational companies are increasingly providing online and remote payment services. This increases the volume of transactions to be examined for detecting suspicious activity and may lead to problems in defining risk. https://www.oecd.org/dataoecd/16/8/35003256.pdfMONEY LAUNDERING & TERRORIST FINANCING TYPOLOGIES, 2004-2005*
- Jim Ensom, 24/05/2007, Financial Crimes Enforcement Network spokeswoman Anne Marie Kelly said, "The bureau is aware of the laundering and terror finance risks posed by emerging payment technologies ... [and have] an ongoing dialogue with the industries involved ... to study and work with [them] in order to provide the law enforcement community with guidance on how these systems operate and the money laundering challenges they may present." However, she did not say how long this "study" will take". Emerging threat from virtual money-laundering, http://www.globalcontinuity.com/current_headlines/emerging_threat_from_virtual_money_laundering

[322] *Jim Ensom, 24/05/2007,"According to Rachel Ehrenfeld, author of "Funding Evil: How Terrorism is Financed and How to Stop It" and John Wood, the president of The Playfair Group, in 2006 online role-playing games had more than 14 million subscribers, generating more than $1 billion in revenues ($576 million in North America and $299 million in Europe)". http://www.globalcontinuity.com/current_headlines/emerging_threat_from_virtual_money_laundering*

وتهدف عمليات الاحتيال والخداع على الانترنت، غالبا، إلى جني الأموال، حيث يستدرج المستخدم إلى افشاء أرقام بطاقة ائتمانه، أو إلى إرسال حوالات مالية أو شيكات، أو إلى اعطاء بياناته الشخصية، ومنها كلمات المرور، إلى حساباته على الانترنت، أو إلى بريده، أو هاتفه الخليوي. ويندرج الاحتيال الذي يستهدف سرقة بطاقات الائتمان، ضمن دائرة خداع الشخص، وسرقة معلوماته، عن طريق الاستخدام الغير مسموح، والغير مشروع، لبيانات البطاقة الائتمانية.

وكان أحد التعاميم الصادرة عن مصرف لبنان، والهادف إلى حماية برامج المعلوماتية، ومكافحة القرصنة، قد نص على "أن الحماية القانونية لبرامج الحاسوب مهما كانت لغاتها، بما في ذلك الأعمال التحضيرية، تخضع للتشريعات المتعلقة بحماية الملكية الفكرية في لبنان، لاسيما قانون الملكية الأدبية والفنية رقم ١٩٩/٧٥.

خلاصات وتوصيات

١ . خلاصات

يشكل ارتباط البنى التحتية الخاصة بتقنيات المعلومات والاتصالات، كما الاعتماد المتزايد عليها، من قبل الدول والأفراد والمؤسسات، عاملا محفزا لتصاعد نسبة المخاطر، ما يفرض اتخاذ تدابير وإجراءات، تضمن إدارة فاعلة للمخاطر التقنية والسيبرانية، تعتمد على منهجية تتناسب والأبعاد الواسعة لهذا الارتباط، ما ينسحب على البلدان اجمع.

لذلك، لا بد ان تنطلق الحلول في هذا المجال، من فهم الطبيعة الخاصة لتقنيات المعلومات والاتصالات، لاسيما الجزء الخاص بتجاوزها للحدود، وللمجتمعات، والأنظمة، كما لطبيعة البنى التحتية نفسها.

على مستوى آخر، تفرض الأبعاد الخاصة بالأمن السيبراني، ارساء قواعد الحماية، على فهم وتصور واضحين وشاملين، للمكونات التقنية والموارد البشرية، بحيث لا تسقط من الحسبان، المخاطر التي يتسبب بها التصرف البشري، سواء أكانت مجرد اخطاء، ام اعمالا جرمية.

على ضوء ما تبين، تجد المخاطر السيبيرانية مصادرها، بشكل أساسي، في أعمال قصدية، أو غير قصدية، وتزداد خطورة متى قابلها قلة وعي وإدراك، لأساليب وطرق الوقاية.

وتفتقر الدول العربية، عامة، إلى موارد بشرية ومالية، كما إلى ارادة واضحة وحازمة، تساعد على متابعة ما يجري في الفضاء السيبراني، من نشاطات غير شرعية، تنطلق من اراضيها. وفي هذا المجال، لا بد من التشديد، على ضرورة التعاون، بين القطاعين العام والخاص والمجتمع المدني، للتوصل إلى نشر ثقافة احترام القانون في الفضاء السيبراني، وحماية الحقوق والحريات الأساسية.

يضاف إلى ذلك، ان البيئة التنظيمية والتشريعية العربية، ما زالت في طور التشكل. وإذا كانت بعض الدول العربية، عضوا في الاتحاد الدولي للاتصالات، وفي الأمم المتحدة، وفي الشراكة الدولية المتعددة الاطراف لمكافحة التهديدات السيبرانية – امباكت –، الا ان الانضمام إلى الجهود الدولية، بحاجة إلى دينامية أكثر فعالية، سواء عبر انضمام المزيد من الدول العربية، إلى الجهود والمنظمات العاملة على برامج أمن وسلامة الفضاء السيبيراني، أو عبر الانضمام إلى المعاهدات الدولية، المعمول بها حاليا.

فلا بد للقوانين ان تحوي قواعد ملزمة، ورادعة، تطاول فيما تطاول، ليس فقط إقرار عقوبات واصول محاكمات وتحقيق خاصة، بل أيضا، مجموعة من الالتزامات القانونية الخاصة بالأمن، كاعتماد المقاييس والمعايير الدولية، الصادرة عن المنظمات والهيئات الدولية المتخصصة، في كل ما يتعلق بحماية الأنظمة المعلوماتية، والبنى التحتية، والبيانات والمعلومات الحساسة. يضاف اليها، اتخاذ الاحتياطات اللازمة، لدفع المسؤولية في حال وقوع اضرار، ناتجة عن نقاط ضعف في البرامج والأنظمة والأجهزة، ولحظ ضرورة الالتزام بمواصفات تقنية، تضمن مصداقية المعلومات والبيانات، في حال اللجوء اليها، أو اعتمادها، في اثبات الأعمال التجارية، والتحويلات المالية، وأي تصرف آخر، يمكن ان يرتب

موجبات ومسؤوليات. الا ان التشريعات العربية، التي ترعى المسائل المتصلة بالأمن والسلامة في الفضاء السيبراني، لا تتلاءم وما تقدم.

وعليه، يلاحظ وجود ثغرات تشريعية في الأنظمة القانونية العربية، لجهة المواضيع التي تتصل بتحقيق الأمن والثقة في الفضاء السيبراني. ويعود ذلك، إلى غياب تشريعي كامل لبعض المواضيع، واللجوء إلى تطبيق القوانين التقليدية في مواضيع اخرى، إضافة إلى تعارض بعض ما أقر من تشريعات، مع الارشادات العالمية أو الممارسات الفضلى، التي تتولى المنظمات الدولية اصدارها.

ويبقى التعاون الشرط الأساس لنجاح هذه المواجهة. وفي هذا المجال، لا بد من إيجاد الإطار التشريعي والتنظيمي الحاضن، الذي يشجيع مبادرات التعاون، اذ ان استمرارية عمل تقنيات المعلومات والاتصالات، وفي مقدمها الانترنت، كما استقرار الفضاء السيبراني، يستدعيان سياسات لمعالجة الثغرات الأمنية، ولمواجهة الأخطار والحد من آثار الأعمال الجرمية. وبالتالي، لا بد من دعم الجهود الآيلة إلى وضع مقاييس ومعايير دولية، كما لا بد من دعم إقرار الاطر القانونية والتنظيمية، والافادة من أفضل الممارسات والتجارب الناجحة، التي تعزز الثقة في الفضاء السيبراني، وتؤمن بيئة داعمة، لنمو النشاط الاقتصادي، والاجتماعي، في الفضاء السيبراني. وفي هذا الإطار، لا بد من الابتعاد عن السياسات، التي تتعارض وطبيعة عمل الانترنت المفتوحة، وامكاناتها التي تشكل أرضية للابداع، والتمو الاقتصادي والاجتماعي، بحيث لا تتحول هذه السياسات، إلى أدوات تعيق الانسياب الحر للمعلومات، والوصول اليها، تحت ذريعة تحقيق الأمن والحماية. لذا، لا بد من الحرص على التالي:

أ- تطوير البنية الادارية

ترتبط الثقة في الفضاء السيبراني، بقدرة الأجهزة المعنية، على ضبط الامور، كما ترتبط، بوضوح المسؤوليات، وتحديد المرجعيات المعنية، بإقرار الحقوق وحمايتها، وبالقدرة على الردع، والملاحقة لكل عمل جرمي، أو تصرف يعرض استقرار المعاملات، والفضاء السيبراني. وتتطلب المكافحة الفاعلة، اجهزة متخصصة، وعناصر تتميز بالكفاءة، والقدرة على الإحاطة بكيفية إدارة أنظمة المعلومات، وطرق معالجة البيانات، والحقوق المتصلة بها. يضاف إلى ذلك، ضرورة وجود مرجعية، تشرف على توثيق الحقوق، وارساء قواعد متينة للثقة في العاملين في مجال معالجة المعلومات، والأنظمة المتصلة بها، كما الحقوق الناشئة عنها، في سجلات خاصة، ذات قيود موثوقة.

من هنا، لا بد من ايلاء عملية بناء قدرات الأجهزة الأمنية، ودوائر تنفيذ القانون، اهمية خاصة. كما لا بد، من إيجاد اجهزة ادارية متخصصة، تتولى اعطاء شهادات خاصة للأشخاص الذين يتولون مراقبة المعلومات، وحفظها، ومعالجتها، كما تتولى تسجيلهم في سجلات خاصة، وتلزمهم بقواعد لحماية المعلومات والأنظمة.

فتشجيع الاستثمار، والابداع، والاختراع، في اسواق العمل المتصلة بوسائل الاتصالات، يرتكز على تحديد واضح للحقوق والموجبات، كما على آليات محددة، لحماية الحقوق الناشئة عن هذا النشاط، كما كان عليه الحال، مع إقرار قوانين الملكية الفكرية، وحقوق المؤلف، والعلامات التجارية، والسجلات التي تثبت الملكية، في عصر ما قبل الانترنت. وفي ذلك أيضا، حفاظ على حقوق المستخدمين، لاسيما حقهم في تطبيق القوانين المرعية الإجراء.

ب- تعزيز وحماية الانسياب العالمي الحر للمعلومات

يرتكز اقتصاد الانترنت، كما نموها، بشكل أساسي، على الانسياب الحر للمعلومات. وإذا كانت الدول المختلفة، مدعوة إلى وضع سياسات تعزز هذا الانسياب، وتشجعه، وتدعمه، الا انها في المقابل، مدعوة أيضا، إلى تامين الإطار القانوني الذي يوفر حماية الحق في الخصوصية، والبيانات الشخصية، والحريات الفردية، وبعض الفئات العمرية، كالأطفال والشباب، والملكية الفكرية. ومن هنا، ضرورة التفاتها إلى الأمن السيبراني، والعمل على ارساء قواعد ثابتة له. ويتصل انسياب المعلومات، بالطبيعة المفتوحة للانترنت، التي تتكل بدورها، على اعتماد مقاييس ومعايير تقنية عالمية. وترد في هذا الإطار أيضا، سياسات المنافسة، والسوق المفتوح، والتنوع، والخدمات العابرة للحدود، التي تسمح بتأمين خدمات، بكلفة معقولة، تساهم في اتاحة الانترنت للجميع.

ج- تشجيع الالتزام بقواعد أخلاقية

يمكن لاي حكومة، ان تقر قواعد قانونية، تدعم وتشجع الالتزام بقواعد اخلاقيات وسلوك معينة، ترافقها آليات محاسبة ومسؤولية خاصة، على غرار ما هو معمول به، في إطار تنظيم بعض المهن، كالتجارة، والطب، والمحاماة، والصحافة، والمصارف، وغيرها. ويمكن لهذه القواعد، ان تساهم في مكافحة التصرفات غير المشروعة، وغير الاخلاقية، كالغش والخداع، والممارسات غير المهنية، كما يمكنها، ان تدعم الحريات العامة، وتحصن الحقوق المعترف بها، في القوانين المرعية الإجراء.

د- الحفاظ على الخصوصية

يعتبر الحفاظ على الحق في الخصوصية، من أساسيات تعزيز الثقة في الفضاء السيبراني، والافادة من طاقات تقنيات المعلومات والاتصالات، على المستويات: الاجتماعية، والاقتصادية، والثقافية. فالتحديات الحالية، التي تطرحها وسائل معالجة البيانات وجمعها، واستخدامها، واستثمارها، لا بد وان تكون ذات انعكاسات سلبية، على استخدام الانترنت، ومروحة التقنيات المتصلة بها، سواء تجاريا، أو اجتماعيا، أو حكوميا. ولابد للاطر التشريعية والتنظيمية، من ان تمكن المستخدمين، من فهم حقيقة ما يجري، من ممارسات تطال بياناتهم الشخصية، والمعلومات التي يضعونها على الانترنت. كما لا بد من تمكينهم، من ممارسة حقوقهم، في ادارتها، بالشكل الذي يطمئنهم إلى امكانية الحفاظ على خصوصيتهم، وعلى حقوقهم الفكرية، والصناعية والادبية. وفي هذا المجال، يمكن للتشريعات، ان تسترشد بالقواعد الدولية، والمبادئ التي سبق إقرارها، على المستوى العالمي، كجزء من أساسيات المحافظة، على نمو واستقرار الفضاء السيبراني[323].

هـ- الاسترشاد بنماذج سابقة

إذا التفتنا إلى الجانب التقني، وصعوبة تحديد المسؤوليات في بعض المسائل، لاسيما منها تلك المرتبطة بالسلامة والأمن، كاختراق البرامج، وسرقة البيانات، وانتشار البرامج الخبيثة، وصعوبات ضبط المحتوى غير المشروع، ومتابعة التصرفات الجرمية، نجد ان بعض القوانين، ذات الطبيعة التقنية،

[323] *OECD guidelines for Privacy*

كالقانون الجوي، والقانون البحري، قد اوجدت حلولا تقنية، طاولت، ليس فقط نوعية قواعدها، وانما أيضا مصادرها. ففي القانون الجوي، تساهم المنظمة الدولية للنقل الجوي (اياتا)، وهي تجمع ذو طابع خاص، في صناعة القانون الجوي، من خلال توليها القواعد الخاصة بمسؤولية الناقل، بينما اوكل امر اعداد وتطوير الملاحق الخاصة بمعاهدة شيكاغو، إلى هيئة تقنية متخصصة، هي المنظمة الدولية للطيران المدني.

اما من حيث المضمون، فقد تولت المعاهدات الخاصة بمنع الاصطدام البحري، وضع قواعد المرور والإشارة، في البحر، مقرة بسلوكيات وتدابير، ذات طبيعة تقنية، يعتبر الخروج عنها، بمثابة خطا معلن للمسؤولية. وعليه، ومراعاة لطبيعة الفضاء السيبراني التقنية، والعالمية والدينامية، يبدو ملحا، التعاون مع الهيئات الدولية الموجودة حاليا، كالاتحاد الدولي للاتصالات، على اعداد ارضية إطار قانوني، يضمن سلامة وأمن الفضاء السيبراني.

كذلك، فقد طورت العديد من قواعد المسؤولية، في مجال النقل البحري، لتنسجم مع التطورات التقنية، التي تمنع مراقبة دقيقة للبضاعة المشحونة، من قبل الناقل، بسبب ظروف العمل، فلحظت آلية لابداء التحفظات، ومبادئ لإقرار صحتها، وتقرير المسؤوليات، ودفعها. كذلك، أقر مبدأ "تحديد مسؤولية مالكي السفن"، تشجيعا للاستثمار في النقل البحري، لاسيما وان مالك السفينة، لا يرافقها، بل يعهد بها، إلى مستثمر أو مجهز. كذلك، وضعت معاهدات، وقواعد سير في البحر، تمكن من تحديد المسؤوليات، عن الصدامات البحرية، في حال حدوثها، ولحظت اتفاقيات خاصة، بمسؤولية الناقلين للمواد الخطرة والنووية، واخرى خاصة بحماية البيئة، ونظمت المناطق البحرية، بحيث احترمت سيادة الدول على جزء من البحار، يمكن للدولة حمايته فعليا، وتركت أعالي البحار، بعيدة عن سيادة اي دولة.

وعليه، ليس ما يمنع، ان تطور قواعد مسؤولية خاصة، تأخذ بعين الاعتبار، جميع الاطراف المعنية، بالحفاظ على استقرار الفضاء السيبراني، من قطاع خاص، مسيطر على البنية التحتية، وموردي خدمات، يتحكمون في الوصول إلى الشبكة العالمية للانترنت، ودولة مسؤولة عن حماية أمنها القومي وأمن مواطنيها، وسلامة مصالحهم، ومستخدمين للشبكة العالمية، معنيين مباشرة بما يضخ من محتوى. كما يمكن وضع أصول عمل، تستند إلى التقنية، واخلاقيات مهنية واجتماعية، تعتبر مخالفتها، أرضية لتحديد المسؤوليات.

٢. توصيات

وختاما، نورد بعض التوصيات، التي يتبناها المرصد العربي للسلامة والأمن في الفضاء السيبراني، واهمها:

- التزام القرارات الصادرة عن الأمم المتحدة، وعن القمة العالمية لمجتمع المعلومات بسقيها، والداعية إلى نشر ثقافة الأمن السيبراني.
- اتخاذ تدابير تعتمد الأمن كعنصر ضروري في الانتاج، لاسيما ما يخص البرامج والأجهزة المستخدمة في تقنيات الاتصال.

- وضع إطار تعاون، يضمن تبادل المعلومات، ونقل الممارسات الفضلى، في المجال الأمني.
- تأمين انسجام الأنظمة القانونية، المكافحة للجرائم السيبرانية، بما يمنع نشوء جنات رقمية.
- وضع استراتيجية لنشر الوعي، وبنائه، لدى مختلف شرائح المجتمع، سواء منهم المستخدمون العاديون، أو المهنيون، أو متخذو القرار، والمسؤولون عن سياسات الأمن والسلامة.
- اعتماد مبادئ خلقية للسلوك السيبراني، على مثال خلفيات واصول التعامل القائمة في المجتمع التقليدي، تكون بمثابة عقد اجتماعي، يؤسس لسلوك يضمن سلامة الجماعة، وسلامة مواردها.
- وضع استراتيجية، وسياسة امنية واضحة وملزمة، لكل المعنيين بصناعة المعلومات، وبإدراة وسائل الاتصالات، والبنى التحتية، كما لاولئك المعنيين بصناعة ادوات وبرامج الاتصال، وخزن المعلومات ومعالجتها. و تحويل الأمن السيبراني، إلى جزء من خطط التنمية والتطوير كافة.
- اخذ جميع أبعاد الأمن السيبراني، بعين الاعتبار، لدى وضع اي استراتيجية أو سياسة، بما في ذلك، حاجات المواطنين والمؤسسات، كما حقوقهم وواجباتهم، بحيث تأتي الخطة متكاملة، ومنسجمة مع ما يمكن توقع الالتزام به، من قبل المعنيين، بأمن مجتمع المعلومات.
- الإقرار بالمسؤولية عن تحقيق الأمن السيبراني، كجزء لا يتجزأ من الأمن القومي والوطني.
- إنشاء مراكز للسلامة المعلوماتية، ولطوارئ الاتصالات، تتعاون فيما بينها، وفق آلية واضحة وشفافة وفاعلة.
- تدريب وتأهيل وحدات عسكرية وامنية خاصة، يمكنها مراقبة البنى التحتية للاتصالات، بحيث تقوم بتحديد المخاطر المحتملة، وازالتها.
- تأهيل وحدات أمنية وعسكرية خاصة، تتولى التعاون على المستوى الخارجي، مع الهيئات العاملة على مكافحة المخاطر، والحد منها ومن آثارها.
- تأهيل الأجهزة القضائية المختصة، والشرطة القضائية، بحيث تتمكن من القيام بواجبها، في مجال ملاحقة ومحاكمة المجرمين السيبرانيين.
- توجيه دعوة من خلال جامعة الدول العربية، إلى دول العالم، لمناقشة إقرار معاهدة دولية، تنطلق ديباجتها من مقررات القمة العالمية لمجتمع المعلومات، مضافا اليها، الإقرار بضرورة عدم تحويل الفضاء السيبراني، إلى مجال يهدد السلم الدولي، مع الالتزام بعدد من المبادئ، وفي مقدمها: مبدأ سيادة الدول، والمساواة فيما بينها، وحق كل دولة في الافادة من قدرات تقنيات المعلومات والاتصالات، بما يضمن قدرتها على المنافسة في هذا المجال، وتحقيق رفاه شعوبها.

إنشاء هيئات تحكيم وطنية، متخصصة في القضايا السيبرانية، وخدمات استشارات، مسبقة ولاحقة لأي نشاط إلكتروني، يمكن لمن يرغب، اللجوء اليها.



الملاحق

ملحق رقم ١ التوصيات عن اللقاء السيبراني الأول ٢٠١٢

ملحق رقم ٢ – التوصيات عن اللقاء السيبراني الثاني ٢٠١٣

ملحق رقم ٣ – التوصيات عن اللقاء السيبراني الثالث ٢٠١٤

ملحق رقم ٤ – التوصيات عن اللقاء السيبراني الرابع ٢٠١٥

ملحق رقم ٥ – ضوابط استخدام الموارد المعلوماتية والاتصالاتية الحكومية

ملحق رقم ٦ – أخلاقيات التعامل مع شبكة الإنترنت

ملحق رقم ٧ – مسودة اتفاقية عربية – بناء الثقة في الفضاء السيبراني

ملحق رقم ١

التوصيات الصادرة عن اللقاء السنوي الأول للمتخصّصين في أمن وسلامة الفضاء السيبراني (الإنترنت) المنعقد في مقر المركز العربي للبحوث القانونية والقضائية

بيروت ٢٧ – ٢٠١٢/٨/٢٨

الموافق ٩– ١٠ شوال ١٤٣٣ هـ

إن المشاركين في اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني (الإنترنت) وانطلاقاً من وعيهم لحجم المخاطر التي قد تصيب بتأثيراتها الأمن القومي السياسي والعسكري والاقتصادي والثقافي العربي والخسائر التي قد تنتج عنها على الصعيد الفردي والجماعي والمؤسساتي.

وإذ يدركون حجم العقبات التي تؤدّي إلى إعاقة التطوّر والتقدّم والرقيّ في المجتمعات العربية.

وإذ يُعربون عن خشيتهم نتيجة لذلك من تلاشي القيم الأخلاقية والقواعد السلوكية. يوصون بما يلي:

أولاً: التأكيد على اعتبار مسألة تحقيق الأمن السيبراني جزءاً لا يتجزّأ من الأمن الوطني والأمن القومي على أساس كونه ركناً أساسياً وقاعدة لنجاح مخططات التنمية والتطوير المجتمعي الوطني والقومي على شتّى الأصعدة وفي مختلف الميادين.

ثانياً: نشر الوعي والمعرفة بحجم المخاطر لدى مختلف شرائح المجتمع والمؤسسات الخاصة والرسمية الناتجة عن التسيّب الأمني في الفضاء السيبراني (الإنترنت) بالإضافة إلى حجم الخسائر وإدراج موضوع أمن وسلامة الفضاء السيبراني في المناهج التعليمية والأكاديمية.

ثالثاً: استنهاض منظمات المجتمع المدني والمؤسسات الرسمية المختصة والتنسيق فيما بينها لتغطية جميع شرائح المجتمع ومؤسساته في الدول العربية فيما يتعلّق بأمن وسلامة الفضاء السيبراني.

رابعاً: وضع قواعد أخلاقية وسلوكية تطال جميع شرائح المجتمع سواء كانوا مستخدمين عاديين أو مهنيين أو متخصّصين أفراداً أو مؤسسات أو متّخذي القرار أو المسؤولين عن سياسات الأمن والسلامة للفضاء السيبراني (الإنترنت) وتكليف الدكتور حسين الغافري من سلطنة عُمان بإعداد مسودة القواعد.

خامساً: الدعوة إلى الاستفادة من تجارب الدول العربية التي عرضت تجاربها خاصة سلطنة عُمان وجمهورية السودان ودولة فلسطين وجمهورية مصر العربية.

سادساً: دعوة الدول العربية لإنجاز البناء التشريعي والقانوني والقضائي بما يضمن المساعدة على مكافحة الجرائم السيبرانية والمعلوماتية وبما يؤمن الانسجام بين كافة الأنظمة القانونية.

سابعاً: إنشاء أجهزة متخصّصة في مجال الأمن السيبراني على مستوى القضاء والنيابات العامة (الإدّعاء العام) والكوادر الفنية والخبراء والمحقّقين، وتأمين التطوير المستمرّ للعاملين في هذه الأجهزة.

ثامناً: إقامة دورات تدريبية متخصّصة بالتعاون بين الدول العربية لكل الجهات والأفراد العاملين في الأجهزة والمؤسسات المعنية بحماية أمن وسلامة الفضاء السيبراني.

تاسعاً: إيجاد الصيغ المناسبة لتأمين التنسيق المتواصل والتعاون الوثيق بين مختلف الأجهزة والمؤسسات الرسمية المعنية بأمن وسلامة الفضاء السيبراني (الإنترنت) على المستويات الوطنية والإقليمية والدولية.

عاشراً: تكليف الدكتورة منى الأشقر جبور بوضع مشروع مسودة إتفاقية عربية لحماية أمن وسلامة الفضاء السيبراني العربي مع مذكرة تتضمن الأسباب الموجبة وعرضها على اللقاء السنوي الثاني.

حادي عشر: تكليف القاضي حاتم جعفر من جمهورية مصر العربية بوضع مسودة مشروع تشريع تنظيمي يؤمّن تنظيم آليات وقواعد للمعنيين بصناعة المعلومات وتخزينها ومعالجتها وكذا المعنيين بصناعة وسائل الاتصالات وإداراتها وبناها التحتية وللمعنيين بصناعة أدوات وبرامج الاتصال والمعلوماتية وحمايتها مع مذكرة تتضمن الأسباب الموجبة وعرضه على اللقاء السنوي الثاني.

ثاني عشر: اعتبار المحاور التالية محاور علمية للقاء السنوي الثاني:

- **أولاً:** واقع البنى التحتية العربية في مجال أمن وسلامة الفضاء السيبراني.
- **ثانياً:** القواعد الأخلاقية والسلوكية الخاصة بأمن وسلامة الفضاء السيبراني.
- **ثالثاً:** إتفاقية عربية لحماية أمن وسلامة الفضاء السيبراني.
- **رابعاً:** التشريع التنظيمي الخاص بأمن وسلامة الفضاء السيبراني.
- **خامساً:** ما يستجدّ من أعمال.

ملحق رقم ٢

التوصيات الصادرة عن المؤتمر الثاني للمتخصّصين في أمن وسلامة الفضاء السيبراني (الإنترنت) المنعقد في مقر المركز العربي للبحوث القانونية والقضائية بيروت ١٩-٢١/٨/٢٠١٣ الموافق ١٢- ١٤ شوال ١٤٣٤ هـ

أولاً: متابعة دراسة مسودة مشروع الاتفاقية العربية لحماية أمن وسلامة الفضاء السيبراني بعد مراجعتها من اللجنة المشكلة من المؤتمر على ضوء الملاحظات الواردة من الدول العربية الأعضاء.

ثانياً: متابعة دراسة مسودة مشروع القواعد والضوابط الأخلاقية لاستخدام الفضاء السيبراني التي أعدّها د. حسين الغافري من قبل اللجنة المشكّلة من المؤتمر على ضوء الملاحظات الواردة من الدول العربية الأعضاء.

ثالثاً: متابعة ما كلّف به د. حاتم جعفر من مصر حول وضع تشريع تنظيم لاستخدام وحماية أمن وسلامة الفضاء السيبراني وتعميمه على المشاركين في المؤتمر الأول والثاني لإبداء ما قد يكون لديهم من آراء وملاحظات حوله.

رابعاً: إيجاد آلية لتفعيل التعاون العربي وتبادل الخبرات والزيارات في مجال حماية أمن وسلامة الفضاء السيبراني.

خامساً: وضع خطط لتفعيل التدريب من خلال التعاون العربي.

سادساً: دعوة الدول العربية لإنشاء هيئة مركزية وطنية مختصة بحماية أمن وسلامة الفضاء السيبراني في الدول التي ليس لها مثل هذه الهيئة تكون من مهماتها تطبيق إجراءات التنظيم والحماية وخاصة البيانات واسترجاعها والتعاون فيما بينها وصولاً إلى تشكيل هيكلية عربية موحدة تؤمن حماية أمن وسلامة الفضاء السيبراني.

سابعاً: دعوة الدول العربية إلى استكمال الأطر التشريعية والبنى التحتية تمهيداً لتشكيل هيئات أو لجان المصادقة والتوقيع الإلكتروني والاستفادة من التجارب العربية في الدول العربية في هذا المجال.

ثامناً: تكليف الدكتور سعيد حيدر من الهيئة الناظمة للاتصالات بإجراء مسح ميداني عربي لمراكز الاستجابة لطوارئ الحاسوب.

تاسعاً: اعتبار المحاور التالية محاور علمية للقاء السنوي الثالث:

أولاً: • دراسة مسودة مشروع الاتفاقية العربية لحماية أمن وسلامة الفضاء السيبراني.

ثانياً: • دراسة مسودة مشروع القواعد والضوابط الأخلاقية لاستخدام الفضاء السيبراني.

ثالثاً: • دراسة مسودة مشروع التنظيم التشريعي لاستخدام وحماية أمن وسلامة الفضاء السيبراني.

رابعاً: • تجارب مراكز الاستجابة لطوارئ الحاسوب Certs في الدول العربية.

خامساً: • ما يستجدّ من أعمال.

ملحق رقم ٣

التوصيات الصادرة عن المؤتمر الثالث للمتخصّصين في أمن وسلامة الفضاء السيبراني (الإنترنت)
المنعقد في مقر المركز العربي للبحوث القانونية والقضائية
بيروت ٢٥ - ٢٠١٤/٠٨/٢٧
الموافق ٢٩ شوال - ١ ذو القعدة ١٤٣٥هـ

أولاً: متابعة دراسة مسودة مشروع الاتفاقية العربية لحماية أمن وسلامة الفضاء السيبراني بعد مراجعتها من المؤتمر على ضوء الملاحظات الواردة من الدول العربية الأعضاء، والطلب إلى الدول التي لم تزوّد المركز العربي بملاحظاتها أن تقوم بذلك بعد إعادة تعميم الاتفاقية مع الردود المستلمة.

ثانياً: الطلب إلى الدول العربية تعميم مسودة الاتفاقية مع الردود والملاحظات المستلمة على الجهات الوطنية المعنية بها في كل دولة حسب ما ترتأيه (الجهات القضائية التشريعية -الأمنية - الاتصالات - إلخ....).

ثالثاً: يطلب من الدول العربية إبداء ملاحظاتها بشكل دقيق يتناول المواد الواردة في الاتفاقية والنص المقترح تعديله أو إلغاءه.

رابعاً: الطلب من الدول العربية دراسة مسودة مشروع القواعد والضوابط الأخلاقية لاستخدام الفضاء السيبراني التي أعدّها د. حسين الغافري وإبداء ملاحظاتها عليه لتعرض في الاجتماع القادم.

خامساً: متابعة ما كلّف به د. حاتم جعفر من مصر حول وضع تشريع تنظيم لاستخدام وحماية أمن وسلامة الفضاء السيبراني وتعميمه على المشاركين في المؤتمر الأول والثاني لإبداء ما قد يكون لديهم من آراء وملاحظات حوله.

سادساً: التأكيد على ضرورة إيجاد آلية لتفعيل التعاون العربي وتبادل الخبرات والزيارات في مجال حماية أمن وسلامة الفضاء السيبراني ووضع خطط لتفعيل التدريب.

سابعاً: التأكيد على التوصيات السابقة بضرورة دعوة الدول العربية لإنشاء هيئة مركزية وطنية مختصة بحماية أمن وسلامة الفضاء السيبراني في الدول التي ليس لها مثل هذه الهيئة تكون من مهماتها تطبيق إجراءات التنظيم والحماية وخاصة البيانات واسترجاعها والتعاون فيما بينها وصولاً إلى تشكيل هيكلية عربية موحدة تؤمن حماية أمن وسلامة الفضاء السيبراني.

ثامناً: التأكيد على دعوة الدول العربية إلى إستكمال الأطر التشريعية والبنى التحتية تمهيداً لتشكيل هيئات أو لجان المصادقة والتوقيع الإلكتروني والاستفادة من التجارب العربية في الدول العربية في هذا المجال.

تاسعاً: اعتبار المحاور التالية محاور علمية للقاء السنوي الرابع:

أولاً:
- دراسة مسودة مشروع الاتفاقية العربية لحماية أمن وسلامة الفضاء السيبراني.

ثانياً:
- دراسة مسودة مشروع القواعد والضوابط الأخلاقية لاستخدام الفضاء السيبراني.

ثالثاً:
- دراسة مسودة مشروع التنظيم التشريعي لاستخدام وحماية أمن وسلامة الفضاء السيبراني.

رابعاً:
- تجارب مراكز الإستجابة لطوارئ الحاسوب Certs في الدول العربية.

خامساً:
- ما يستجدّ من أعمال.

ملحق رقم ٤

التوصيات الصادرة عن المؤتمر الرابع للمتخصّصين في أمن وسلامة الفضاء السيبراني (الإنترنت)
المنعقد في مقر المركز العربي للبحوث القانونية والقضائية
بيروت ١٧ – ٢٠١٥/٠٨/١٩
الموافق ٢ – ٤ القعدة ١٤٣٦هـ

أولاً: متابعة دراسة مشروعيّ الاتفاقية العربية لحماية أمن وسلامة الفضاء السيبراني والتشريع التنظيمي النموذجي للأمن السيبراني بعد مراجعة ذلك من المؤتمر على ضوء الملاحظات الواردة من الدول العربية الأعضاء، والطلب إلى الدول التي لم تزوّد المركز العربي بملاحظاتها أن تقوم بذلك خلال فترة لا تتجاوز شهر مطلع شهر سبتمبر، على أن يقوم المركز بإعداد جداول مقارنة بالتعديلات وإرسالها إلى الدول العربية.

ثانياً: الأخذ بعين الاعتبار الملاحظات والتعديلات المقترحة على مشروع الاتفاقية والمقدّمة من كل من سلطنة عُمان والسودان وفلسطين خلال المؤتمرات السابقة وما يستجدّ من بقية الدول.

ثالثاً: يُرجى من الدول العربية إبداء ملاحظاتها بشكل دقيق يتناول المواد الواردة في الاتفاقية والنص المقترح تعديله أو إلغاءه. وكذا نشروا التشريع التنظيمي بعد قيام المركز العربي بتعميم ما تمّ الانتهاء منه من تكليفات سابقة.

رابعاً: استكمال اجتماعات المؤتمر الرابع في موعد يحدّد في ضوء استكمال الردود على أن يعقد قبل منتصف أكتوبر.

خامساً: التمني على الدول العربية تزويد المركز العربي للبحوث القانونية والقضائية بالقوانين أو مشاريع القوانين الخاصة بحماية وسلامة الفضاء السيبراني.

سادساً: التمني على الدول العربية استكمال دراسة مسودة مشروع القواعد والضوابط الأخلاقية لاستخدام الفضاء السيبراني التي أعدّها د. حسين الغافري وإبداء ملاحظاتها عليه لتعرض في الاجتماع القادم.

سابعاً: الحثّ على إيجاد آلية لتفعيل التعاون العربي وتبادل الخبرات والزيارات في مجال حماية أمن وسلامة الفضاء السيبراني ووضع خطط لتفعيل التدريب.

ثامناً: التأكيد على التوصيات السابقة بضرورة دعوة الدول العربية لإنشاء مراكز إستجابة لطوارئ الحاسب وهيئة مركزية وطنية مختصة بحماية أمن وسلامة الفضاء السيبراني في الدول التي ليس لها مثل هذه الهيئات.

تاسعاً: اعتبار المحاور التالية محاور علمية للقاء الخامس القادم:

أولاً: • استكمال دراسة مسودة مشروع الاتفاقية العربية لحماية أمن وسلامة الفضاء السيبراني.

ثانياً: • استكمال دراسة مسودة مشروع القواعد والضوابط الأخلاقية لاستخدام الفضاء السيبراني.

ثالثاً: • استكمال دراسة مسودة مشروع التنظيم التشريعي لاستخدام وحماية أمن وسلامة الفضاء السيبراني.

رابعاً: • عرض تجارب مراكز الاستجابة لطوارئ الحاسوب Certs في الدول العربية.

خامساً: • ما يستجدّ من أعمال.

ملحق رقم ٥

ضوابط استخدام الموارد المعلوماتية والاتصالاتية الحكومية

١ . تعريفات

في تطبيق أحكام هذه الضوابط يكون للكلمات والعبارات المعنى المحدد قرين كل منها ما لم يقتض سياق النص خلاف ذلك:

- الشخص: أي شخص ذي صفة طبيعية، أو اعتبارية عامة أو خاصة.
- المستخدم: الشخص المصرح له باستخدام الأنظمة المعلوماتية.
- حساب المستخدم: البيانات السرية التي تخول المستخدم استخدام الأنظمة المعلوماتية، وتتكون في حدها الأدنى من أسم مستخدم وكلمة المرور.
- الحاسب الآلي: أي جهاز إلكتروني ثابت أو منقول، سلكي أو لا سلكي، يحتوي على نظام معالجة البيانات، أو تخزينها، أو إرسالها أو استقبالها، أو تصفحها، ويؤدي وظائف محددة بحسب البرامج، والأوامر المعطاة له.
- برامج الحاسب الآلي: مجموعة معلومات إلكترونية أو تعليمات تستعمل بطريقة مباشرة أو غير مباشرة في نظام معالجة معلومات إلكترونية بغرض الوصول إلى نتائج محددة.
- الأنظمة المعلوماتية أو الموارد المعلوماتية: مجموعة برامج أو أدوات أو معلومات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الآلية.
- البيانات أو المعلومات الإلكترونية: كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات أيا كان شكله كالكتابة والصور والأصوات والرموز والإشارات.
- البيانات أو المعلومات الرسمية: البيانات أو المعلومات الصادرة من الجهات الحكومية ذات الطابع الرسمي.
- الوثائق: البيانات المستخدمة لأغراض متعددة كالنماذج والخطابات والعقود والإحالات والتقارير والدراسات.
- التعاملات الإلكترونية: أي تبادل أو تراسل أو تعاقد، أو أي إجراء آخر يبرم أو ينفذ – بشكل كلي أو جزئي – بوسيلة إلكترونية.
- الإنترنت: الشبكة العالمية للمعلومات
- الشبكة المعلوماتية: ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البينات وتبادلها ، مثل الشبكات الخاصة والعامة وشبكة الانترنت.

- الموقع الإلكتروني: مكان إتاحة المعلومات الإلكترونية على الشبكة المعلوماتية من خلال عنوان محدد.
- البريد الإلكتروني العام: هو البريد الإلكتروني غير المقدم من جهة حكومية.

ـ الضوابط:

أ. يجب على المستخدمين المصرح لهم باستخدام الموارد المعلوماتية والاتصالاتية التقيد بجميع السياسات والإجراءات الخاصة بالأنظمة المعلوماتية التي يستخدمونها.

ب. يجب على مستخدمي موارد الاتصالات والمعلومات في أي جهة حكومية باستخدامها بشكل مثمر ومسؤول ولأغراض تخص العمل فقط، ولا يجوز استخدامها لأغراض شخصية أو أغراض تخالف القوانين واللوائح المعمول بها في السلطنة، أو بما يؤدي إلى الإضرار بالجهة الحكومية أو بسمعتها، ويشمل ذلك على سبيل المثال لا الحصر:

١. استخدامها في أي عمل أو غرض غير شرعي.

٢. استخدمها بما يتعارض مع الأخلاق والآداب العامة.

٣. الدخول إلى حسابات المستخدمين أو محاولة استخدامها دون تصريح.

٤. اشراك الآخرين في أي من حسابات الاستخدام أو التنازل لهم عن تلك الحسابات.

٥. استخدام الخدمة أو استغلالها بطريقة تعرض الشبكة الداخلية للخطر أو فتح ثغرات أمنية في الشبكة أو نشر برمجيات ضارة أو غير ذلك.

٦. تثبيت أو نشر برامج حاسب آلي غير مخول بها من قبل الجهة الحكومية وبدون الحصول على تصريح مسبق بذلك.

٧. نشر مواد أو بيانات سرية خاصة بالمؤسسة أو أية مؤسسة حكومية أخرى دون التخويل من قبل الجهة الحكومية صاحبة البيانات وبدون إجراءات أمنية مناسبة تضمن سرية تلك البيانات.

٨. انتحال شخصية شخص أو جهاز آخر.

٩. العبث بالمعلومات الخاصة بموظفين آخرين أو الاطلاع عليها.

١٠. نشر المعلومات الشخصية أو الخاصة بالآخرين دون تصريح بذلك.

١١. محاولة فك تشفير بيانات الآخرين في الأنظمة المعلوماتية.

١٢. الإخلال بأي من حقوق النشر أو التأليف، أو حقوق الملكية الفكرية لأي بيانات أو معلومات.

١٣. مراقبة الاتصالات الإلكترونية للمستخدمين (التجسس)

١٤. الاستخدام بشكل يؤثر سلبيا على المستخدمين الآخرين، أو على أداء الأجهزة والشبكات

١٥. الاستخدام الذي من الممكن أن يتسبب في أي تهديد، أو تخريب، أو إزعاج أو اهانة، أو مضايقة لأي شخص أو جهة أو أمنها الإلكتروني مثل إرسال بريد إلكتروني بشكل متكرر، أو غير مرغوب فيه أو لغرض الغش أو لخداع الآخرين.

١٦. إحداث أي تغيير في الموارد المعلوماتية أو الاتصالاتي الحكومية دون امتلاك صلاحية.

١٧. إنشاء موقع إلكتروني يمثل المنشأة الحكومية، أو إدارته، دون إذن كتابي رسمي من صاحب الصلاحية.

١٨. استخدام الموارد المعلوماتية والاتصالاتية لأغراض شخصية لا تخص جهة العمل أو بشكل يؤدي إلى إهدارها وإهدار وقت الموظف.

ج. عدم استخدام قنوات اتصال بالموارد المعلوماتية والاتصالاتية الحكومية أو الارتباط بها، إلا من خلال القنوات المتاحة من قبل الجهة الحكومية.

د. يعتبر المستخدم مسؤولا مسؤولية كاملة عن كل ما يصدر من استخدام لجهازه أو من خلال الحاسب الخاص به، وعليه الحرص على الدخول للموارد المعلوماتية المنوطة به.

هـ. تعد المراسلات عن طريق البرد الإلكتروني الحكومي ملكا للجهة الحكومية وللجهة الحكومية المتخصصة حق الاطلاع على تلك المراسلات وفقا للقانون في حالة وجود تحقيق رسمي.

ملحق رقم ٦

أخلاقيات التعامل مع شبكة الإنترنت

١ . مقدمة

التكنولوجيا بجميع أشكالها وأنواعها من أجهزة حواسيب وشبكة انترنت وهواتف محمولة عادية وذكية وكاميرات رقمية وألعاب الفيديو، وجدت لتسهل وتيسر للإنسان والمجتمع حياته ورفاهيته. لكن الواقع الحالي يؤكد عكس ذلك فهناك من يجهل أو يتجاهل الأهداف الأساسية من اختراع وتطوير هذه التكنولوجيات، كما لا يعرف كيفية استخدامها استخداما أخلاقيا سليما، والمثال على ذلك، الاستخدام غير الأخلاقي لشبكة الإنترنت، من اعتداء على الخصوصيات والتجسس المعلوماتي وسرقة الهويات الشخصية وانتهاك حقوق الملكية الفكرية، وسرقة البعض للنتاج الفكري للآخرين من بحوث ومقالات ونسبها لأنفسهم، أو سرقة الأرصدة والأموال البنكية عبر التحويل الإلكتروني، أو سرقة البرامج أو إعادة نسخها، أو إتلاف وإزالة وتشويه البيانات والمعلومات أو التلاعب بها ، أو التخريب والتدمير الإلكتروني للأنظمة المعلوماتية أو الترويج لمواد ومحتويات ضارة غير هادفة عبر رسائل البريد الإلكتروني أو من خلال المواقع الإلكترونية أو غرف المحادثة ، أو في الإساءة إلى أشخاص وتلويث وتشويه سمعتهم، ناهيك عن المخاطر التي تنجم عن التحاور مع الآخرين عبر مواقع المحادثة أو ما يسمى بغرف الدردشة (الشات). وكذلك من يستخدمون الهواتف المحمولة لإزعاج الآخرين بالمعاكسات أو نشر صور مخلة بالآداب عبر كاميرات هذه الهواتف أو استخدامها في نشر الشائعات.

في ظل كل ذلك ظهرت الحاجة إلى إيجاد مجموعة من المبادئ والأخلاق تجعل من وسائل تقنية المعلومات والاتصالات بكافة أنواعها وسائل فعالة راقية للاتصال وتبادل المعلومات والمعرفة النافعة. وهي غير مرتبطة بوسائل تقنية المعلومات والاتصالات كوسائل في حد ذاتها وإنما متعلقة بالمستخدم ذاته الذي يعقل أفعاله. ولا تتعلق بالأنظمة التي تقنن استخدام وسائل تقنية المعلومات بقدر ما هي متعلقة بالخلق الموجود في نفوسنا الذي سيحكم كيفية تصرفنا عندما لا يكون هناك نظام مفروض.

وقد تكون هذه الأخلاقيات بين الفرد المستخدم للتكنولوجيا ونفسه أو بينه وبين الآخرين، هذا بالإضافة إلى أخلاقيات بين المستخدم والمكونات المادية للتكنولوجيا، والتي تشمل الحرص على سلامة الأجهزة ومحتوياتها من التكسير والإتلاف.

٢ . الضوابط والأحكام

أخلاقيات التعامل مع وسائل تقنية المعلومات والاتصالات قد تكون بين الفرد المستخدم للتكنولوجيا ونفسه، وقد تكون بينه وبين الآخرين، هذا بالإضافة إلى أخلاقيات بين المستخدم والمكونات المادية

للتكنولوجيا، والتي تشمل الحرص على سلامة الأجهزة ومحتوياتها من التكسير والإتلاف

إذن نستطيع أن نقسم أخلاقيات التعامل مع وسائل تقنية المعلومات والاتصالات إلى ثلاثة أقسام على النحو التالي:

القسم الأول ـ أخلاقيات التعامل بين الفرد المستخدم للتكنولوجيا ونفسه:

ينبغي على أي مستخدم لأي وسيلة من وسائل تقنية المعلومات أو الاتصالات وهو بصدد استخدام هذه التكنولوجيا أن يراعي:

أ. تقوى الله ومراقبته والإيمان الصادق بأن الله يعلم السر وأخفى.

ب. أن تتفق استخداماته مع تعاليم الأديان السماوية.

ت. احترام الذات والقيم والمبادئ والعادات والتقاليد.

ث. تجنب الدخول إلى المواقع المشبوهة الضارة والالتزام بالمواقع التي تتناسب مع العمر وتحقق الأهداف وتحقق الحاجات.

القسم الثاني ـ أخلاقيات التعامل بين المستخدم للتكنولوجيا وغيره من المستخدمين :

- يتعين على مستخدمي التكنولوجيا التعريف بأنفسهم بشكل واضح وصريح في كل المراسلات والاتصالات الإليكترونية حيث يعتبر إخفاء الهوية أو إخفاء الانتماء الإداري أو انتحال شخصية الغير تصرفات منافية للأخلاق.
- احترام الاخرين واحترام افكارهم وارائهم وعدم السخرية منهم وتجنب الاساءة إليهم أو جرح مشاعرهم عند التواصل معهم عبر وسائل تقنية المعلومات والاتصالات وتجنب التحاور الإلكتروني عندما يكون جدلا بلا غاية.
- توخ الدقة والمباشرة والايجاز في طرح الافكار ومحاورة الاخرين.
- الابتعاد عن التزوير والخداع.
- مراعاة حقوق النشر أو التأليف، وحقوق الملكية الفكرية لأي بيانات أو معلومات..
- تجنب انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم.
- عدم استخدام وسائل تقنية المعلومات في إرسال رسائل إلكترونية لغير أصحابها، ومراعاة ضرورة توجيه رسالة اعتذار عند ارسال مثل هذه الرسائل لغير اصحابها.
- التعامل بأمانة مع الوثائق الإلكترونية التي تصل خطا إلى عنوان البريد الإلكتروني واعادتها على الفور إلى مرسلها وعدم استغلالها الاستغلال السيئ.
- تجنب ارسال الرسائل المسلسة – رسالة يبعث بها إلى مجموعة من الاشخاص على التوالي ويقوم كل فرد من المجموعة بإعادة ارسالها إلى مجموعة اخرى وفي معظم الاحيان يغلب على هذه النوعية من المراسلات تفاهة المحتوى وتسبب هدرا للوقت ولموارد الشبكة.
- تجنب الاضرار بالاخرين عن طريق ارسال البرامج الضارة لأجهزتهم وأنظمتهم المعلوماتية.

- تجنب التعرض لتعاليم الأديان جميعا بسوء والابتعاد عن تجريح الرموز الدينية أو الهيئات أو الدول أو الشعوب وعدم اثارة النعرات والحميات المذهبية أو الطائفية.
- تجنب الاستخدام الذي من الممكن أن يتسبب في أي تهديد، أو تخريب، أو إزعاج أو إهانة، أو مضايقة لأي شخص مثل إرسال بريد إلكتروني بشكل متكرر، أو غير مرغوب فيه أو لغرض الغش أو لخداع الآخرين.
- تجنب نشر ما من شأنه بث الكراهية التي تشجع وتروج للقضاء على مجموعة معينة أو أي تصوير يشين أو يحقر أو يشوه سمعة شخص أو مجموعة على أساس الجنس والعرق والدين والجنسية والتوجه الجنسي أو الاعاقة.
- تجنب نشر ما من شأنه تعريض أمن الناس أو صحتهم أو سلامتهم للخطر.
- تجنب نشر أو توفير محتوى غير لائق ومخل بالآداب، وخصوصا التعري والجنس.
- تجنب نشر أي إساءة لذوي الإعاقة الجسدية أو العقلية أو الحسية.

القسم الثالث ـ أخلاقيات التعامل بين المستخدم وبين التكنولوجيا ذاتها:

- تجنب التقاط غير المشروع للمعلومات أو البيانات.
- تجنب استخدام وسيلة اتصالات غير مرخصة محليا في التقاط الشبكة مثل الالتقاط المباشر من الأقمار الصناعية أو نحوها.
- تجنب اتلاف أو تغيير أو محو أية بيانات أو معلومات بدون وجه حق.
- تجنب التقاط أو تسجيل أو جمع البيانات أو المعلومات وإعادة استخدامها بشكل غير قانوني.
- تجنب التقاط مواد من شأنها المساس بالأخلاق والآداب العامة أو تتعارض مع عقيدة المجتمع وقيمه.
- تجنب سرقة رموز خدمة الآخرين أو استغلالها.
- تجنب اختراق الأنظمة لغرض سرقة المعلومات، أو الأموال أو أي عمل آخر مخالف للقانون.

تجنب استخدام اللغة السيئة بما في ذلك عبارات الازدراء والكلمات النابية والشتائم وفاحش القول. وتتضمن اللغة السيئة اللغة الجارحة ويقصد استخدام كلمات الاساءة أو الاستهزاء التي تسيئ للآخرين. والإشارات الغليظة.

ملحق رقم ٧

مسودة اتفاقية عربية
بناء الثقة في الفضاء السيبراني

١ . الديباجة

يسجل في العالم العربي، نقص في الاطر التشريعية الملائمة، لحماية الفضاء السيبراني، ما يؤثر سلبا على الانخراط السليم في مجتمع المعلومات والمعرفة، ما يستدعي تضافر جهود الدول العربية، لوضع الاطر التشريعية والتنظيمية، التي تسمح لها، بالتعاون الفاعل، لرفع التحديات التي تترافق والتحولات الجذرية التي ادخلتها تقنيات المعلومات والاتصالات، على الحياة اليومية للمواطنين، والمؤسسات، والحكومات، والمنظمات الاقليمية والدولية، لاسيما وان معظم الدول العربية، ما زالت تفتقر إلى الادوات التشريعية، والتنفيذية، والتقنية، والهيكلية، والبشرية، يضمن سلامة مواطنيها وأمنها القومي

فالأنظمة المعلوماتية، ووسائل الاتصالات، مفتوحة ويمكن الولوج اليها، عن بعد، ومن اي مكان في العالم، وقد تحولت بما تحويه وتنقله، من بيانات ومعلومات، وما تؤمنه من خدمات، إلى هدف للمجرمين، وللاستخبارات، والتجسس بكل أنواعه، كما باتت الاعتداءات على الشبكة العالمية للمعلومات، تهدد استمرارية الحكومات، كما تعرض السلام والأمن الدوليين للخطر.

على ضوء هذا الواقع، تبدو الحاجة ملحة، إلى تأمين أدوات الحماية، ووسائل فاعلة، لإدارة المخاطر التقنية، والمعلوماتية، والقانونية، ذات الأبعاد العالمية، ما يستدعي انخراط الدول العربية، في مسيرة تحقيق حماية الفضاء السيبراني، لتأمين مصالحها الاقتصادية، والثقافية، والأمنية، والاجتماعية، مع الحفاظ على الحقوق الأساسية للمواطنين والأفراد، وحماية حرياتهم، لاسيما حياتهم الخاصة.

ونظرا للأبعاد المتعددة والمعقدة للأمن السيبراني، لا بد من الاخذ بعين الاعتبار، كل التشعبات التقنية، والاقتصادية، والسياسية، والاجتماعية، وذلك على جميع المستويات، من خلال التزام استراتيجية واضحة، تلحظ تحقيق مستوى من الحماية التقنية للبنى التحتية للاتصالات، تساعد على السيطرة على المخاطر، وبناء مجتمع معلومات يحترم القيم الانسانية، وسلامة الانسان والأموال، وحقوق الملكية الفكرية والادبية.

وادراكا منها لهذه المخاطر، ورغبة منها، في تعزيز التعاون فيما بينها، لبناء الثقة في مجتمع المعلومات، والحفاظ على الأمن القومي وسلامة المواطنين، في مواجهة الأخطار التي تواكب استخدامات تقنيات المعلومات والاتصالات، والتي يمكن أن تهدد أمن الأمة العربية واستقرارها، ومصالحها الحيوية. والتزاما منها، بالمبادئ الأخلاقية والدينية السامية، و بالتراث الإنساني للأمة العربية القائم على مبادئ الانفتاح، والتعاون، واحترام الفكر، و حماية حقوق الإنسان، بما ينسجم مع مبادئ القانون الدولي

وقواعده التي قامت على تعاون الشعوب من أجل إقامة السلام.

والتزاما منها، بميثاق جامعة الدول العربية وميثاق هيئة الأمم المتحدة، وجميع العهود والمواثيق الدولية الأخرى، التي تكون الدول المتعاقدة في هذه الاتفاقية، طرفا فيها.

وتأكيدا منها، على حق الشعوب في النفاذ إلى المعرفة، والافادة من الإمكانات الهائلة لتقنيات المعلومات والاتصالات، في تحقيق أهداف الالفية وذلك وفقا لمقررات القمة العالمية لمجتمع المعلومات، ولمقاصد ومبادئ ميثاق وقرارات الأمم المتحدة.

وانسجاما مع القرارات الصادرة عن الهيئة العامة للامم المتحدة، والداعية إلى نشر ثقافة الأمنفي الفضاء السيبراني، والحفاظ على سلامة البيانات، وحماية البنية التحتية لتقنيات المعلومات والاتصالات، ومكافحة الجريمة السيبرانية.

ولما كانت تقنيات المعلومات والاتصالات، تشكل عصبا حيويا لنشاط الفردي والحكومي، بأوجهه كافة، الاجتماعية، والاقتصادية، والتعليمية، والتنموية، والمالية

ولما كانت التطورات المتسارعة في المجال السيبراني، وطبيعتها التقنية العالية، تتطلب خبرات، وتبادل معارف، وتقنيات متطورة، ومتابعة دولية، تفترض تضافر جهود عدد من الدول، لانجاح خطوات الحفاظ على السلامة والأمن، والملاحقة الفاعلة، وتطبيق القوانين، ومنع تحول الفضاء السيبراني إلى جنات للجريمة

ولما كانت دول العالم وحكوماته، متفقة، على أن التسخير الايجابي، لطاقات وقدرات تقنيات المعلومات والاتصالات، يشكل عنصرا حيويا في تحقيق رفاه شعوبها.

ولما كانت الحكومات المجتمعة في القمة العالمية لمجتمع المعلومات، بمرحلتيها، قد اقرت ضرورة تحقيق الثقة في مجتمع المعلومات، في مواجهة الأخطار الهائلة التي تواكب بروز الفضاء السيبراني، والتي تنعكس سلبا على أمن الأفراد، والأمن القومي

ولما كانت الدول المجتمعة، راغبة في تحقيق الثقة في الفضاء السيبراني، سعيا إلى ضمان انخراط سليم في مجتمع المعلومات، مع إقرارها بضرورة حماية حقوق وحريات الأفراد، والمواطنين، والمؤسسات، والحد من انعكاسات الممارسات الجرمية، والاعتداءات، والهجومات عليها، عبر الفضاء السيبراني

ولما كانت طبيعة الانترنت، ووسائل الاتصال، وبنيتها التحتية، متسمة بالعالمية، وبالقدرة على عبور الحدود، والربط بين الأفراد، والمؤسسات، والحكومات، والمنظمات، الخاضعة لسيادات مختلفة

ولما كانت الشبكة العالمية للمعلومات، قد تحولت إلى هدف للاعتداءات الجرمية الفردية، والمنظمة.

ولما كانت الجريمة المنظمة والإرهابيون، يلجأون إلى استخدام تقنيات الاتصالات والمعلومات، في التخطيط والاعداد لاعمالهم الجرمية، ونشاطاتهم المختلفة.

ولما كانت تقنيات الاتصالات والمعلومات، تتجاوز عددا من حدود الدول، فلقد أصبح ضروريا ان تقر كل دولة، إطارا تشريعيا ملائما، يمكن الركون اليه، في ملاحقة الجرائم السيبرانية العابرة للحدود، سواء

لناحية التجريم، أو لناحية الملاحقة والتحقيق وتسليم المجرمين وإقرار التعويضات، وإنزال العقوبات الرادعة بشكل فاعل.

ولما كانت الاعتداءات والأعمال الجرمية، الحاصلة على الشبكة العالمية للاتصالات، وعلى بنيتها التحتية، ذات انعكاسات كارثية، على المستويات الاقتصادية، والاجتماعية، والسياسية، والمالية، والدفاعية، والأمنية.

ولما كان من الافضل، تلافي اسباب النزاعات، التي يمكن ان تنشأ بين الدول العربية أو بين شعوبها، وتعزيز الانفتاح والتفاهم والتلاقي، فيما بينها، تحقيقا للتعاون، بما ينسجم مع عدم تهديد السلام العربي، والاقليمي، والعالمي.

ولما كانت الدول العربية المجتمعة تقر، بالحاجة إلى التعاون، لضبط الجوانب السلبية لاستخدامات تقنيات المعلومات والاتصالات، وبضرورة التنسيق والعمل المشترك، وحشد الجهود، لتحقيق السلامة، والأمن، والثقة، وحفظ السلام، في الفضاء السيبراني، ومنع تحوله إلى أرضية خصبة للنزاعات بكل أشكالها.

لذا ، اتفقت الدول العربية المجتمعة، على وضع هذه الاتفاقية، الموقعة أدناه، داعية من لم تكون طرفا فيها، إلى الانضمام اليها. والتزمت تحقيق الغايات المرجوة منها.

٢. السياق

انطلاقا من واقع البيئة التشريعية والتنظيمية في المنطقة العربية، التي تظهر نقصا، وقصورا عن تأمين الإطار الملائم، لمواجهة التحديات الناشئة، عن افلاش استخدامات تقنيات المعلومات والاتصالات، على جميع المستويات، ونظرا، للحاجة الملحة إلى حماية الفضاء السيبراني، من خلال إقرار الاطر القانونية المناسبة، والمنسجمة، التي تضمن الثقة في الفضاء السيبراني، وفي الاقتصاد الرقمي، وتطور مجتمع المعرفة، عبر تنظيم مسائل تنظيم التجارة الإلكترونية، والمعاملات والعقود الإلكترونية، وحماية البيانات ذات الطابع الشخصي، والبيانات الحساسة، ومكافحة الجرائم السيبرانية، وحماية الملكية الفكرية، والصناعية، وجميع حقوق المؤلف، والحقوق المجاورة،

تلتزم الدول الأعضاء، العمل معا، على المستوى العربي، ومنفردة، على المستوى الوطني، لإقرار التشريعات التي تتناسب ومتطلبات الانخراط السليم والأمن في مجتمع المعرفة، وتمنع بروز جنات جرمية سيبرانية، وتمنع تحولها إلى منصة، للاعتداء على الدول الاخرى، العربية منها والاجنبية.

٣. الأهداف

تهدف الاتفاقية، إلى المساهمة في الحفاظ على القوى الوطنية والعربية، والثروات الانسانية والمالية، والتقنية، والمعلوماتية، للافراد والمؤسسات والحكومات. ولذلك، لا يتوقف نطاق الاتفاقية عند حدود سلامة وحماية الفضاء السيبراني، في مواجهة الجريمة السيبرانية، بل يتعداه إلى الى ضرورة تنظيم

التجارة الإلكترونية، والمعاملات الإلكترونية، وحماية البيانات الشخصية، والبنية التحتية، والرد على المخاطر التي تهدد استمرارية المؤسسات والحكومات، وانسياب المعلومات، في حال تحققها، وتأمين امكانية الرجوع السريع، إلى ممارسة النشاط، بأقل خسارة ممكنة، وبكلفة معقولة، ووضع آليات قانونية وقضائية، تضمن ممارسة الأفراد لحقوقهم، في الفضاء السيبراني.

٤ . تعريفات

الأمن القومي:

هو قدرة الامة على الدفاع عن أمنها، وحقوقها، وصياغة استقلالها، وسيادتها على اراضيها، وتنمية القدرات والإمكانات العربية، في مختلف المجالات السياسية، والاقتصادية، والثقافية والاجتماعية، مستندة إلى القدرة العسكرية، والدبلوماسية، آخذة في الاعتبار الاحتياجات الأمنية الوطنية لكل دولة، والإمكانات المتاحة، والمتغيرات الداخلية، والاقليمية، والدولية، والتي تؤثر على الأمن القومي العربي.

الفضاء السيبراني:

هو الفضاء الذي اوجدته تكنولوجيا المعلومات والاتصالات، وفي مقدمها الانترنت. ويرتبط هذا الفضاء، ارتباطا وثيقا بالعالم المادي، عبر البنى التحتية المختلفة للاتصالات، والأنظمة المعلوماتية، وعبر العديد من الخدمات، التي لم يكن بالامكان الحصول عليها، من دونه، وليس اقل ذلك، الوصول إلى البيانات والمعلومات.

تقنيات المعلومات والاتصالات:

هي تطبيق التقنيات الإلكترونية، ومنها الحاسب الآلي، والاقمار الصناعية، وغيرها من التقنيات المتقدمة، كالحوسبة السحابية، لاقتناء وانتاج المعلومات التناظرية والرقمية، وتخزينها واسترجاعها، وتوزيعها، ونقلها من مكان إلى آخر، بواسطة أجهزة تعمل إلكترونيا، وتجمع بين أجهزة الحاسب الآلي، وأجهزة الاتصال من بعد.

البنية التحتية:

هي الأجهزة والمعدات، المستخدمة للربط بين أجهزة الحاسب الآلي، وبين هذه الأخيرة ومستخدميها. وتشمل البنية التحتية وسائل الإعلام، بما في ذلك خطوط الهاتف، وخطوط تلفزيون الكابل، والأقمار الصناعية والهوائيات، وكذلك أجهزة التوجيه (Routers)، والتجميع (Aggregators)، وغيرها من الأجهزة التي تتحكم في مسارات الإرسال. كما تشمل أيضا، البرامج التي يتم استخدامها لتوليد الخدمات المرتبطة بها، وذات العلاقة بتلك (التقنية) التي تصاحبها، والبرمجيات العامة، وخدمات التطوير والصيانة المرتبطة بها، وخطوط التشبيك، التي تربط بين تلك البرمجيات.

الحوسبة السحابية:

هي تقنية تأمين النفاذ، إلى بنية تحتية مشتركة لخدمات الاتصالات والمعلومات، كالشبكات، والمخدمات، والتطبيقات، ومخازن البيانات، والتي يمكن توفيرها وتامينها، بأقل قدر من تدخل مورد الخدمات.

متعهدو الخدمات:

يقصد بهم، اي شخص أو مجموعة، تؤمن للمشتركين معه أو معها، خدمات الاتصال، بواسطة تقنيات المعلومات والاتصالات، عن طريق اجهزة الكومبيوتر، أو غيرها من الأجهزة التي يمكن الاتصال من خلالها، بالشبكة العالمية للمعلومات، أو بشبكات داخلية، وأي شخص أو مجموعة، تعالج البيانات، أو تخزنها، لصالح متعهدي خدمات الاتصال، أو مستخدمي هذه الخدمات.

المنشآت الحرجة:

هي مجموعة الشبكات والأنظمة، التي ترتبط بمنشآت، أو قطاعات، أو مؤسسات، أو ادارات، أو افراد، بما فيها كل شبكات توزيع الخدمات والمنتجات الضرورية للدفاع، والأمن الاقتصادي، وعمل الحكومة واجهزتها المختلفة، على كل المستويات، بشكل سليم، مثال: الاتصالات، الطاقة، الصحة، القطاع المالي والمصرفي، النقل، الصحة، المياه، الخ...

البيانات:

جميع المصطلحات، والرموز، والحروف، والصور والارقام، التي تدخل إلى النظام المعلوماتي، بشكل معين، لتحويلها إلى معلومة.

البيانات الشخصية:

هي البيانات العائدة إلى شخص معين، والتي يمكن ان تساعد على تحديد هويته، والتعرف اليه، كالاسم الشخصي، وعنوان السكن، ورقم الهاتف، والبريد الإلكتروني، ورقم السيارة، وغيرها.

البيانات الحساسة:

هي البيانات الشخصية، التي تكشف الافكار السياسية، أو المعتقدات الدينية والفلسفية، أو الحالة الصحية والنفسية، أو الميول الجنسية، أو السوابق الجنائية، أو العرق، أو التركيبة الجينية، وكل ما يمكن أن يؤثر في رأي المطلع على المعلومات، بشكل يؤدي إلى التمييز العنصري، بكل أشكاله.

المعلومات:

هي مجموع البيانات، التي تسمح بمعرفة معينة، أي كل ما ينتج عن عملية جمع البيانات، وتحليلها، او معالجتها، ووضع الملاحظات والتسجيلات عليها، وكل العمليات، التي تؤدي إلى التمكين من الاجابة على بعض الاسئلة، حول هذه البيانات.

عمليات التشفير

كل عملية تهدف إلى انتاج، استخدام، استيراد، تصدير، وتسويق أدوات التشفير.

المصادقة

هي الاعتراف الرسمي، بان البرنامج أو النظام، يؤمن الحد المطلوب من الحماية والأمن، بناء على معايير تحددها هيئة رسمية، معترف بها.

الترميز chiffrement

هي عملية تحويل البيانات الرقمية، إلى بيانات غير مقروءة، باستخدام تقنيات التشفير.

التجارة الإلكترونية

نشاط اقتصادي، يمارس باستخدام تقنيات المعلومات والاتصالات، سواء أكان عرض خدمات، أو بيع أموال، أو إعلانات، أو تقديم معلومات، أو المساعدة في الحصول عليها.

الاتصال الإلكتروني بالجمهور

كل اتصال إلكتروني، ذي طابع غير خاص، يضع في متناول الجمهور، علامات، أو اشارات، نصية، أو تصويرية، أو صوتية.

اتفاقية سرية

تعني المفاتيح غير المعلنة، والضرورية، لتنفيذ عملية تشفير، أو فك تشفير.

البريد الإلكتروني

هي كل رسالة نصية، صوتية، أو تصويرية، مرسلة عبر شبكة اتصال عامة، محفوظة على مخدم للشبكة، أو في تجهيزات المرسل اليه.

التوقيع الإلكتروني

هو بيانات، أو اشارات، أو آليات مدمجة، في مستند إلكتروني، ومضافة اليه، أو مرتبطة بها منطقيا، تستخدم لتحديد هوية الموقع على المعاملة، أو المستند، ولتأكيد موافقته على محتوى المعاملة، أو المستند.

التشفير

هو علم حماية البيانات وأمنها، لاسيما أوجه سريتها، والتحقق منها، وسلامتها، وعدم ردها. la non répudiation

المعلومات

هي كل عنصر معرفي يمكن تمثيله باستخدام تقنيات المعلومات بهدف استخدامه، حفظه، معالجته، أو

توزيعه ونشره. والمعلومة يمكن ان تكون نصية، تصويرية، صوتية، رقمية الخ..

٥. المبادئ

المادة الأولى:

تقر الدول العربية، المنضمة إلى الاتفاقية، بسيادة كل دولة عربية، وحقها في تطبيق أنظمتها وقوانينها المرعية الإجراء، في مجال ضبط الفضاء السيبراني، ضمن إطار التعاون، لتحقيق أهداف هذه الاتفاقية.

المادة الثانية:

تلتزم الدول العربية الأعضاء، استخدام طاقاتها ومواردها، في مجال تقنيات المعلومات والاتصالات، بما ينسجم مع أهداف هذه الاتفاقية، ومع سياسة منع تحول الفضاء السيبراني، إلى مركز انطلاق لعمليات عسكرية، أو إستخباراتية، أو تخريبية، أو عدائية، أو حربية، ضد الدول الأعضاء في هذه الاتفاقية، وذلك بما يتماشى، مع ضرورات الحفاظ على السلامة العامة، والأمن القومي.

المادة الثالثة:

تمتنع الدول العربية الأعضاء، عن استخدام تقنيات المعلومات والاتصالات، ضد الدول الاخرى، بشكل يتعارض مع تحقيق أهداف الاتفاقية، وتتعهد بعدم تنظيم، أو تمويل، أو تشجيع الاعتداءات علىيها، أو الاشتراك فيها، تحت أي مسمى، ما لم يكن في إطار من التعاون العربي، وكجزء من منظومة دفاعية، في مواجهة اعتداءات على مؤسساتها، أو على مواطنيها.

المادة الرابعة:

تطبق هذه الاتفاقية، على كل المسائل الناشئة، عن النزاعات والخلافات، نتيجة الاستخدام المسيئ، لتقنيات الاتصالات والمعلومات.

المادة الخامسة:

تعترف الدول المتعاقدة، بحق كل دولة عربية، في النفاذ إلى الفضاء السيبراني.

٦. حماية البنية التحتية والمنشآت الحرجة

المادة السادسة:

تتعهد الدول المتعاقدة، أن تأخذ بعين الاعتبار، التدابير اللازمة، لحماية المنشآت الحرجة، ولضمان سلامة البنية التحتية للاتصالات والمعلومات، عند إنشاء، أو وضع تجهيزات تقنيات الاتصالات والمعلومات، أو لدى ابرام عقود توكيل، خاصة بإدارة البنية التحتية للاتصالات، ومنشآتها، أو خدمات الاتصال الإلكترونية.

المادة السابعة:

تلزم الدول المتعاقدة، الجهات الخاصة التي تتعاقد معها، لإدارة المنشات الحرجة، والبنية التحتية على المستوى الوطني، أو تنشئها، أو تؤهلها، أو تعدها، ان تتقيد بالمعايير الدولية والعربية، المرعية الإجراء، في مجال ضمان السلامة والأمن، في الفضاء السيبراني

المادة الثامنة:

تمتنع الدول المتعاقدة، عن اللجوء إلى إجراءات تعطل الاتصالات، أو تضر بالمنشآت الحرجة، وبالبنية التحتية لها، أو تعرض أمن وسلامة الفضاء السيبراني، ومصالح الأفراد والدول، لأي خطر كان.

المادة التاسعة:

يحق لكل دولة، أن تلجأ إلى اعتراض أي عمل تخريبي، أو إرهابي، يستهدف المنشآت الحرجة، أو يضر بالبنية التحتية لتقنيات المعلومات والاتصالات، على ان تنسجم الوسائل التي تستخدمها، مع الآليات المحددة لمواجهة الأخطار، والتي تقرها المنظمة العربية للفضاء السيبراني.

المادة العاشرة:

تلزم الدول الأعضاء في الاتفاقية، جميع الشركات، والمؤسسات الخاصة والعامة لديها، المعنية بتأمين خدمات الاتصالات، بالتوجيهات والمعايير الخاصة بالسلامة والأمن، التي تقرها المنظمة العربية لسلامة الفضاء السيبراني.

كما تلتزم، أن تقر القواعد القانونية الملائمة، التي تجعل من مخالفة هذه التوجيهات والمعايير جرما يعاقب عليه بعقوبات شديدة، وفقا لقانونها الداخلي، وبحسب الاصول التشريعية والتنظيمية الوطنية.

المادة الحادية عشرة:

يعود لكل دولة، أن تتخذ التدابير التقنية، والتنظيمية، والقانونية المناسبة، لحظر الاستخدام الجرمي المتعمد، لتقنيات المعلومات والاتصالات، انطلاقا من أراضيها، ومن الاقليم الخاضع لسيادتها، بما يمنع استخدام الفضاء السيبراني، لاغراض تتنافى مع مقاصد هذه الاتفاقية، ومقتضيات التعاون.

٧. التعاون

المادة الثانية عشرة:

تتعاون الدول الأعضاء، مع الهيئات الدولية والاقليمية، المتخصصة في قضايا حماية الفضاء السيبراني، لاسيما منها اللجان التابعة للامم المتحدة، والاتحاد الدولي للاتصالات، والآيكان (هيئة الانترنت للأسماء والارقام)، وجامعة الدول العربية، وهيئات الاتحاد الأوروبي، ومجموعة دول الكومنولث، ومنظمة التعاون والتنمية الاقتصادية، وأي هيئة دولية أخرى ذات اختصاص وصلة بمسائل الأمن السيبراني، ترى ضرورة للتعاون معها.

المادة الثالثة عشرة:

تتعاون الدول المتعاقدة، لبناء الثقة في الفضاء السيبراني، والخدمات الإلكترونية، ولمكافحة ومنع الجرائم السيبرانية، طبقا للقوانين والإجراءات الداخلية لكل دولة منها، من خلال الآتي:

أولا- تبادل المعلومات:

١. تتعهد الدول المتعاقدة، بتعزيز تبادل المعلومات فيما بينها، حول:

- نشطة وجرائم الجماعات، التي تنظم اعتداءات وهجمات، على أنظمة المعلومات، والبنية التحتية للاتصالات والمعلومات، والمواقع، وحول من يكشف من عناصرها، وأماكن انطلاق الأعمال الجرمية، ووسائل ومصادر وأنواع الفيروسات التي تستخدمها، وغيرها من وسائل الاعتداء، والاعتداء على المواقع، واقفالها، أو السيطرة عليها، وتحوير المعلومات، وتحويل الاتصالات.
- مواقع هذه الجماعات، ووسائل الاتصال والدعاية التي تستخدمها، وأساليب عملها.
- نقاط الضعف، التي تكشف في التطبيقات الحكومية والفردية

٢. تتعهد كل من الدول المتعاقدة، بأخطار أية دولة متعاقدة أخرى، على وجه السرعة، بالمعلومات المتوفرة لديها، عن أي جريمة سيبرانية، أو اعتداء يستهدف المساس بمصالح تلك الدولة، أو بموطنيها، على أن تبين تلك الأخطار، ما أحاط بالجريمة من ظروف، وأسماء الجناة ، والضحايا، والخسائر الناجمة عنها، والأدوات والأساليب المستخدمة في ارتكابها، وذلك بالقدر الذي لا يتعارض، مع متطلبات البحث والتحقيق.

٣. تتعهد الدول المتعاقدة، بالتعاون فيما بينها، لتبادل المعلومات لمكافحة الجرائم السيبرانية، والمبادرة إلى أخطار الدولة أو الدول الأخرى المتعاقدة، بكل ما يتوافر لديها من معلومات، أو بيانات، من شأنها أن تحول دون وقوع الاعتداءات والهجمات السيبرانية، على إقليمها، أو ضد مواطنيها، أو المقيمين فيها، أو ضد مصالحها.

٤. تتعهد كل من الدول المتعاقدة، بتزويد أية دولة متعاقدة أخرى. بما يتوافر لديها من معلومات، أو بيانات، من شأنها:

أ. أن تساعد في القبض على متهم، أو متهمين بارتكاب جريمة سيبرانية، ضد مصالح تلك الدولة، أو الشروع، أو الاشتراك فيها، سواء بالمساعدة، أو الاتفاق، أو التحريض.

ب. بأن تضبط أية أجهزة، أو برامج، أو تطبيقات، أو معدات اتصال طرفية، استخدمت، أو أعدت للاستخدام، في جريمة سيبرانية.

٥. تتعهد الدول المتعاقدة، بالمحافظة على سرية المعلومات المتبادلة فيما بينها، وعدم تزويد أية دولة غير متعاقدة، أو جهة أخرى ، دون أخذ الموافقة المسبقة، للدولة مصدر المعلومات.

ثانيا- التحريات:

تتعهد الدول المتعاقدة، بتعزيز التعاون فيما بينها، وتقديم المساعدة، في مجال إجراءات التحري، والقبض على الهاربين من المتهمين، أو المحكوم عليهم بجرائم سيبرانية، وفقا لقوانين وأنظمة كل دولة.

ثالثا– تبادل الخبرات:

١. تتعاون الدول المتعاقدة، على إجراء وتبادل الدراسات والبحوث، كذلك الخبرات، لمكافحة الجرائم السيبرانية.

٢. تتعاون الدول المتعاقدة، في حدود إمكاناتها، على توفير المساعدات الفنية المتاحة، لإعداد برامج، أو عقد دورات تدريبية مشتركة، أو خاصة بدولة، أو بمجموعة من الدول المتعاقدة، عند الحاجة، للعاملين في مجال مكافحة الجريمة السيبرانية، لتنمية قدراتهم العلمية والعملية، ورفع مستوى أدائهم.

المادة الرابعة عشرة:

على الدول الأعضاء، إنشاء هيئات خاصة، توكل إليها مهمة متابعة طوارئ الانترنت، وتبادل المعلومات، فيما يخص هذه الطوارئ، والرد عليها، ونشر المعلومات حولها، مثل مراكز الاستجابة لطوارئ الانترنت.

٨. التعاون في المجال الأمني

المادة الخامسة عشرة:

تلتزم الدول المتعاقدة التعاون، في اتخاذ تدابير منع ومكافحة جميع الجرائم السيبرانية، بما فيها الجريمة المنظمة، لاسيما منها الجرائم السيبرانية الإرهابية، وتبييض الأموال.

المادة السادسة عشرة:

تتعهد الدول المتعاقدة، بالتزام المعايير والمقاييس الخاصة، بضمان حماية الفضاء السيبراني، وبضمان أمن المعلومات، والأنظمة المعلوماتية، والبنية التحتية، وكافة وسائل الاتصالات، وباتخاذ التدابير التقنية، والقانونية، والتنظيمية، التي تضمن آليات ردع فاعلة، وتعزز سبل المكافحة، لمنع ومواجهة الاعتداءات والأعمال الجرمية، التي يمكن ارتكابها ضدها أو عبرها، وذلك بما ينسجم، مع قوانينها الداخلية، وأنظمتها المعتمدة.

فقرة أولى: تدابير المنع

- التعاون والتنسيق، بين الأجهزة المتخصصة، في الدول المتعاقدة
- دعم الجهود الخاصة، بتطوير وتعزيز الأنظمة المتصلة بالكشف المبكر عن الاعتداءات، وطوارئ الانترنت
- تأهيل، وتطوير، وتعزيز الكفاءات والقدرات المؤسساتية والفردية، عبر برامج تدريبية، وبناء قدرات، للحد من خطورة العنصر البشري، في حصول الاعتداءات.
- تعزيز نظم تأمين أنظمة المعلومات، وحماية البيانات الشخصيات، والمنشآت الحرجة، ووسائل الاتصالات، بأشكالها كافة.

- التعاون مع المنظمات الإقليمية والدولية المتخصصة، وذات الصلة، المعتمدة لدى الدولة المتعاقدة، وفقا للقوانين الداخلية لكل دولة، وللاتفاقيات الدولية، التي تحكم هذا الموضوع
- تعزيز أنشطة التوعية والإعلام الأمني، وتنسيقها مع الأنشطة الإعلامية، في كل دولة، وفقا لسياستها الإعلامية، بهدف تعزيز الوعي لدى الأفراد، والمؤسسات والادارات، في القطاعين العام والخاص، وإحباط مخططات الاعتداء، وبيان مدى خطورتها، على الأمن والاستقرار.
- تقوم كل دولة، بإنشاء قاعدة بيانات، لجمع وتحليل المعلومات، الخاصة بالاعتداءات، والجرائم السيبرانية، ومخترقي الأنظمة، والجماعات والحركات والتنظيمات، المتخصصة في هذا المجال، ومتابعة مستجدات ظاهرة الاعتداء، على الشبكة العالمية للمعلومات، والبنية التحتية الخاصة بها، وتحديد نقاط الضعف، في الأنظمة والتطبيقات المعلوماتية، والتجارب الناجحة في مواجهتها، وتحديث هذه المعلومات، وتزويد الأجهزة المختصة في الدول المتعاقدة بها، وذلك في حدود ما تسمح به القوانين، والإجراءات الداخلية، لكل دولة.
- إنشاء مراكز وطنية حكومية، لطوارئ الانترنت، وتشجيع جميع الجهود، الرامية إلى إنشاء مراكز مشابهة، لدى مؤسسات القطاعين العام والخاص، على ان تلتزم التوجيهات والسياسات الوطنية الخاصة، وتتعاون مع المراكز الوطنية.
- تعمل الدول المتعاقدة، على اتخاذ تدابير فاعلة، لمنع انتشار الفيروسات، والبرمجيات الخبيثة، والتطبيقات المؤذية، ولمنع الأنشطة غير الشرعية، على الشبكة العالمية للاتصالات، وكل طرفيات الاتصال. وتحقيقا لهذه الغاية، تبقى الدول المتعاقدة، على تشاور وثيق فيما بينها، ومع الوكالات الدولية المعنية بالتدابير الاحترازية، ووسائل الحماية التقنية.
- تتعهد الدول المتعاقدة، أن تتعاون لبلوغ أقصى درجة ممكنة من الانسجام، في الأنظمة والمعايير والإجراءات والتنظيم، فيما يتعلق بأمن وسلامة الأنظمة المعلوماتية، والبيانات الشخصية، والمعلومات، والبنية التحتية، والمنشآت الحرجة، والأفراد، ومساعدة المستثمرين في قطاع المعلومات والاتصالات، ومتعهدي الخدمات، في جميع المسائل التي يطاولها هذا التعاون، على تحقيق الانسجام، لاسيما منها، مسألة تعزيز الثقة، في الاقتصاد الرقمي. Une telle consultation ne préjuge en rien l›application de toute convention internationale existant en la matière et à laquelle les Etats contractants seraient parties.

فقرة ثانية: تدابير المكافحة:

- القبض على مرتكبي الجرائم، المعلوماتية والسيبرانية، ومحاكمتهم وفقا للقانون الوطني، أو تسليمهم وفقا لأحكام هذه الاتفاقية، أو الاتفاقيات الثنائية، بين الدولتين، المعنيتين، بعملية القاء القبض
- تأهيل العاملين في مجال الملاحقة، والمكافحة، والمحاكمة، في الجرائم المعلوماتية، والسيبرانية. إقامة تعاون فاعل، بين الأجهزة المعنية، وبين المواطنين، لمواجهة الاعتداءات على الشبكة العالمية للمعلومات، ووسائل الاتصال الاخرى، والبنية التحتية ، بما في ذلك نشر الوعي، حول خطورة هذه الاعتداءات، وأهمية الابلاغ عنها، في الحد من آثارها السلبية، وإيجاد ضمانات وحوافز مناسبة، للتشجيع على الإبلاغ عن الاعتداءات، والاختراقات، وتقديم المعلومات التي تساعد في الكشف عنها، والتعاون في القبض على مرتكبيها.

- إقرار اتفاقيات خاصة، تسمح بالملاحقة عبر الحدود، وبتسليم المجرمين، بين الدول الأعضاء في الاتفاقية، وبين الدول الأعضاء، والدول الاجنبية.
- وضع أسس تعاون، مع المؤسسات العاملة في القطاع الخاص، تضمن تسليم وتبادل المعلومات، حول النشاطات المشبوهة، والنشاطات الجرمية، في الوقت الملائم، لنجاح المكافحة والملاحقة.
- تتعهد كل دولة، بالاستجابة الفورية، لكل طلب معلومات، حول عمليات اعتداء، أو اختراق، أو توزيع فيروسات، يطاول الأنظمة المعلوماتية لديها، سواء أكان ذلك، في اداراتها ومؤسساتها، أو لدى المقيمين لديها، او المواطنين.
- للسلطات المختصة، في كل دولة، الحق في بدء عمليات تتبع، وطلب معلومات، والحصول عليها، عن كل خطر أو اعتداء، لاسيما متى كان هذا الخطر، أو الاعتداء، يطال منشآتها الحرجة، أو يعرض أمنها القومي للخطر.
- تتعهد الدول، ان تقدم عند الطلب، من أي دولة عضو، أو من المنظمة العربية للسلامة والأمن في الفضاء السيبراني، معلومات كافية، عن أية جهة لديها، يمكن ان تشكل مصدر الخطر، أو الاعتداء الحاصل، وذلك، بحسب الاصول القانونية الوطنية.
- عند تهديد أمن وسلامة الاتصالات، والبنية التحتية، والمنشآت الحرجة، في أي من الدول المتعاقدة، أو عند وقوع اعتداء على احداها، تتعهد الدول المتعاقدة، بالتحقيق في ظروف الخطر، أو الاعتداء، بقدر ما تسمح به قدراتها وقوانينها، وبالتعاون مع المنظمة العربية للسلامة والأمن في الفضاء السيبراني، وبابلاغ نتائج التقرير، إلى الدول المعنية بالخطر، أو الاعتداء، سواء مباشرة، أو بواسطة المنظمة.

٩. التعاون القضائي

المادة السابعة عشرة:

تقدم كل دولة متعاقدة، للدول الأخرى، المساعدة الممكنة واللازمة، لتحقيقات أو إجراءات المحاكمة، المتعلقة بالجرائم السيبرانية.

المادة الثامنة عشرة:

يجوز للدولة المتعاقدة، صاحبة الصلاحية القضائية، في محاكمة متهم عن جريمة سيبرانية، أن تطلب إلى الدولة، التي يوجد المتهم في إقليمها، محاكمته عن هذه الجريمة، شرط موافقة هذه الدولة، وشرط ان تكون الجريمة، معاقبا عليها في دولة المحاكمة، بعقوبة سالبة للحرية، لا تقل مدتها عن سنة واحدة، أو بعقوبة أخرى أشد. وتقوم الدولة الطالبة، في هذه الحالة، بتزويد الدولة المطلوب منها، بجميع التحقيقات، والوثائق، والأدلة، الخاصة بالجريمة. تطبق في التحقيق، أو المحاكمة، في هذه الحال، الأحكام والإجراءات الخاصة بدولة المحاكمة.

المادة التاسعة عشرة:

يترتب على تقديم الدولة الطالبة لطلب المحاكمة، وفقا للمادة السابقة، وقف إجراءات الملاحقة، والتحقيق، والمحاكمة، المتخذة لديها بشأن المتهم المطلوب محاكمته، باستثناء ما تستلزمه مقتضيات التعاون، أو المساعدة، أو الإنابة القضائية، التي تطلبها الدولة المطلوب إليها، إجراء المحاكمة.

المادة العشرون:

أ. تخضع الإجراءات التي تتم في أي من الدولتين – الطالبة، أو التي تجرى فيها المحاكمة– لقانون الدولة التي يتم فيها الإجراء، وتكون لها الحجية المقررة، في هذا القانون.

ب. لا يجوز للدولة الطالبة، محاكمة أو إعادة محاكمة، من طلبت محاكمته، إلا إذا امتنعت الدولة المطلوب إليها، عن إجراء محاكمته.

ج. وفي جميع الأحوال، تلتزم الدولة المطلوب منها المحاكمة، بأخطار الدولة الطالبة، بما اتخذته بشأن طلب إجراء وبنتيجة التحقيقات، أو المحاكمة التي تجريها.

المادة الواحدة والعشرون:

للدولة المطلوب إليها إجراء المحاكمة، اتخاذ جميع الإجراءات والتدابير، المنصوص عنها في تشريعاتها، تجاه المتهم، سواء في الفترة، التي تسبق وصول طلب المحاكمة إليها، أو بعده.

المادة الثانية والعشرون:

لا يترتب على نقل الصلاحية في المحاكمة، المساس بحقوق المتضررين من الجريمة. ويكون لهم، حق اللجوء إلى قضاء الدولة الطالبة، أو دولة المحاكمة، للمطالبة بحقوقهم المدنية، والتعويضات التي يستحقونها، والناشئة عن الجريمة.

المادة الثالثة والعشرون:

يتم تبادل طلبات التسليم، بين الجهات المختصة، في الدول المتعاقدة، مباشرة، أو عن طريق وزارات العدل، أو من يقوم مقامها، أو بالطريق الدبلوماسي.

المادة الرابعة والعشرون:

يقدم طلب التسليم كتابة، أو بواسطة وسائل الاتصال الإلكترونية، المعتمدة بين الدولتين، أو الدول المتعاونة، مصحوباً بما يلي:

١. أصل حكم الإدانة، أو أمر القبض، أو أية أوراق أخرى، لها القوة نفسها، والصادرة طبقاً للأوضاع المقررة في قانون الدولة الطالبة، أو صورة رسمية عما تقدم.

٢. بيان بالأفعال المطلوب التسليم من أجلها، يوضح فيه: زمان ومكان ارتكاب الافعال، ووصفها القانوني، مع الإشارة إلى المواد القانونية المطبقة عليها، وصورة عن هذه المواد.

٣. بيانات وأوصاف الشخص المطلوب تسليمه، بأكبر قدر ممكن من الدقة، وأية بيانات أخرى، من شأنها تحديد شخصه، وجنسيته وهويته.

المادة الخامسة والعشرون:

للسلطات القضائية في الدولة الطالبة، أن تطلب من الدولة المطلوب إليها– بأي طريق من طرق الاتصال، الكتابية أو الإلكترونية، وقف الشخص احتياطيًا، إلى حين وصول طلب التسليم.

ويجوز في هذه الحالة، للدولة المطلوب إليها التسليم، أن توقف الشخص المطلوب احتياطيًا. وإذا لم يقدم طلب التسليم، مصحوبًا بالمستندات اللازمة المبينة في المادة السابقة، فلا يجوز توقيف الشخص المطلوب تسليمه، مدة تزيد على ثلاثين يومًا، تبدأ من تاريخ إلقاء القبض عليه، أو مدة تزيد عن المدة المحددة في القانون الوطني، للدولة منفذة عملية التوقيف.

المادة السادسة والعشرون:

على الدولة الطالبة، أن ترسل طلبًا مصحوبًا بالمستندات اللازمة، المنصوص عنها في هذه الاتفاقية. وبعد ان تتحقق الدولة، المطلوب إليها التسليم سلامة الطلب، تتولى السلطات المختصة فيها، تنفيذه طبقًا لتشريعاتها الوطنية، على أن تبلغ الدولة الطالبة، دون تأخير، بما اتخذ بشأن طلبها.

المادة السابعة والعشرون:

إذا رأت الدولة المطلوب إليها التسليم، حاجة إلى إيضاحات تكميلية، للتحقق من توافر الشروط، المنصوص عليها في هذه الاتفاقية، تبلغ بذلك الدولة الطالبة، وتحدد لها موعدا، لاستكمال هذه الإيضاحات.

المادة الثامنة والعشرون:

إذا تلقت الدولة المطلوب إليها، عدة طلبات تسليم، من دول مختلفة، إما عن الأفعال ذاتها، أو عن أفعال مختلفة، يكون لها، أن تفصل في هذه الطلبات، مراعية الظروف كافة، وعلى الأخص إمكان التسليم اللاحق، وتاريخ وصول الطلبات، ودرجة خطورة الجرائم، والمكان الذي ارتكبت فيه.

المادة التاسعة والعشرون:

أ. إذا تقرر تسليم الشخص المطلوب تسليمه، تلتزم أي من الدول المتعاقدة، بضبط وتسليم الأشياء، والعائدات المتحصلة من الجريمة السيبرانية، أو المستعملة فيها، أو المتعلقة بها، للدولة الطالبة، سواء وجدت في حيازة الشخص المطلوب تسليمه، أو لدى الغير. وتلتزم الدول بالتسليم، ولو لم يتم تسليم الشخص المقرر تسليمه، بسبب هربه، أو وفاته، أو لأي سبب آخر، وذلك بعد التحقق، من أن تلك الأشياء، متعلقة بالجريمة السيبرانية.

ب. لا تؤثر هذه الأحكام، على حقوق أي من الدول المتعاقدة، أو الاشخاص الثالثين، حسني النية، في ملكيتهم للأشياء أو العائدات المذكورة.

المادة الثلاثون:

للدولة المطلوب إليها، تسليم الأشياء والعائدات، اتخاذ جميع التدابير، والإجراءات التحفظية، اللازمة

لتنفيذ التزامها بتسليمها. ولها أيضا، أن تحتفظ مؤقتا بهذه الأشياء أو العائدات، إذا كانت لازمة، لإجراءات جزائية تتخذ عندها، أو أن تسلمها إلى الدولة الطالبة، بشرط استردادها منها، للسبب عينه.

المادة الواحدة والثلاثون:

تتعهد الدول المتعاقدة، بفحص الأدلة، والآثار الناتجة عن أية جريمة سيبرانية، تقع انطلاقا من إقليمها، ضد دولة متعاقدة أخرى، بواسطة أجهزتها المختصة. ولها الاستعانة، بأية دولة متعاقدة أخرى في ذلك. وتلتزم باتخاذ الإجراءات اللازمة، للمحافظة على هذه الأدلة والآثار، واثبات دلالتها القانونية، ولها وحدها الحق في تزويد الدولة، التي وقعت الجريمة ضد مصالحها، بالنتيجة، متى طلبت ذلك، ولا يحق للدولة، أو الدول المستعان بها، أخطار أية دولة بذلك.

١٠. تسليم المجرمين

المادة الثانية والثلاثون:

تتعهد كل من الدول المتعاقدة، بتسليم المتهمين، أو المحكوم عليهم، في الجرائم السيبرانية، المطلوب تسليمهم، من أي من هذه الدول، وذلك طبقا للقواعد والشروط، المنصوص عليها في هذه الاتفاقية.

المادة الثالثة والثلاثون:

لا يجوز التسليم، في أي من الحالات الآتية:

أ. إذا كانت الجريمة، المطلوب من أجلها التسليم، معتبرة، بمقتضى القواعد القانونية النافذة لدى الدولة المتعاقدة، المطلوب إليها التسليم، جريمة ذات صبغة سياسية.

ب. إذا كانت الجريمة، المطلوب من اجلها التسليم، تنحصر في الإخلال بواجبات عسكرية.

ج. إذا كانت الجريمة، المطلوب من أجلها التسليم، قد ارتكبت في إقليم الدولة المتعاقدة المطلوب إليها التسليم، إلا إذا كانت هذه الجريمة، قد أضرت بمصالح الدولة المتعاقدة، طالبة التسليم، وكانت قوانينها، تنص على تتبع مرتكبي هذه الجرائم، ومعاقبتهم، ما لم تكن الدولة المطلوب إليها التسليم، قد بدأت إجراءات التحقيق، أو المحاكمة.

د. إذا كانت الجريمة، قد صدر بشأنها حكم نهائي، له صفة القضية المبرمة، لدى الدولة المتعاقدة المطلوب إليها التسليم، أو لدى دولة متعاقدة ثالثة.

ه. إذا كانت الدعوى، عند وصول طلب التسليم، قد انقضت، أو العقوبة قد سقطت، بمضي المدة، طبقا لقانون الدولة المتعاقدة، طالبة التسليم.

و. إذا كانت الجريمة، قد ارتكبت خارج إقليم الدولة المتعاقدة الطالبة، من شخص لا يحمل جنسيتها، وكان قانون الدولة المتعاقدة، المطلوب إليها التسليم، لا يجيز توجيه الاتهام عن مثل هذه الجريمة، إذا ارتكبت خارج إقليمه، من مثل هذا الشخص.

ز. إذا صدر عفو، يشمل مرتكبي هذه الجرائم، لدى الدولة المتعاقدة الطالبة.

ح. إذا كان النظام القانوني، للدولة المطلوب إليها التسليم، لا يجيز لها تسليم مواطنيها، فتلتزم الدولة المطلوب إليها التسليم، بتوجيه الاتهام، ضد من يرتكب منهم، لدى أي من الدول المتعاقدة الأخرى، جريمة من الجرائم السيبرانية؛ إذا كان الفعل معاقبا عليه، في كل من الدولتين، بعقوبة سالبة للحرية، لا تقل مدتها عن سنة، أو بعقوبة أشد. وتحدد جنسية المطلوب تسليمه، بتاريخ وقوع الجريمة، المطلوب التسليم من أجلها، ويستعان في هذا الشأن، بالتحقيقات التي أجرتها الدولة، طالبة التسليم.

المادة الرابعة والثلاثون:

إذا كان الشخص المطلوب تسليمه، قيد التحقيق، أو المحاكمة، أو محكوما عليه، عن جريمة أخرى، في الدولة المطلوب إليها التسليم، فان تسليمه يؤجل، لحين التصرف في التحقيق، أو انتهاء المحاكمة، أو تنفيذ العقوبة، ويجوز مع ذلك، للدولة المطلوب إليها التسليم، تسليمه مؤقتا، للتحقيق معه، أو محاكمته، بشرط إعادته للدولة، التي سلمته، قبل تنفيذ العقوبة عليه، في الدولة طالبة التسليم.

١١. الإنابة القضائية

المادة الخامسة والثلاثون:

لكل دولة متعاقدة، أن تطلب إلى أية دولة أخرى متعاقدة، القيام في إقليمها، نيابة عنها. بأي إجراء قضائي، متعلق بدعوى ناشئة عن جريمة سيبرانية، وبصفة خاصة.

أ. سماع شهادة الشهود، والأقوال التي تؤخذ، على سبيل الاستدلال.

ب. تبليغ الوثائق القضائية.

ج. تنفيذ عمليات التفتيش والحجز.

د. إجراء المعاينة، وفحص الأشياء.

ه. الحصول على الأدلة الثبوتية، الإلكترونية منها، والتقليدية.

المادة السادسة والثلاثون:

يجب أن تتضمن، طلبات الإنابة القضائية، البيانات الآتية:

- الجهة المختصة، الصادر عنها الطلب.
- موضوع الطلب، وسببه.
- تحديد هوية الشخص المعنى بالإنابة، وجنسيته، قدر الإمكان.
- بيان الجريمة التي تطلب الإنابة بسببها، ووصفها القانوني، والعقوبة المقررة لها، و أكبر قدر ممكن من المعلومات عن ظروفها، بما يؤمن دقة تنفيذها.

المادة السابعة والثلاثون:

يوجه طلب الإنابة القضائية، مباشرة من السلطات القضائية، في الدولة الطالبة، إلى السلطات القضائية، في الدولة المطلوب إليها. وترسل صورة من هذه الإنابة، في الوقت عينه، إلى وزارة العدل في الدولة المطلوب إليها، وتعاد مصحوبة، بالأوراق المتعلقة بتنفيذها، بالطريق نفسه.

كما يمكن، توجيه طلب الإنابة القضائية، مباشرة من الجهات القضائية، إلى الجهة المختصة في الدولة المطلوب إليها، ويجوز أن تحال الردود، مباشرة عن طريق هذه الجهة.

المادة الثامنة والثلاثون:

ويتوجب أن تكون طلبات الإنابة القضائية، والمستندات المصاحبة لها، موقعًا عليها، ومختومة بخاتم سلطة مختصة، أو معتمدة منها. وتعفى هذه المستندات، من كافة الإجراءات الشكلية، التي قد يتطلبها، تشريع الدولة المطلوب إليها.

المادة التاسعة والثلاثون:

إذا كانت الجهة، التي تلقت طلب الإنابة القضائية، غير مختصة بمباشرته، تعين عليها، إحالته تلقائيًا، إلى الجهة المختصة في دولتها، وفى حالة إرسال الطلب بالطريق المباشر، فإنها تحيط الدولة الطالبة، علمًا بالطريقة نفسها.

المادة الأربعون:

لا يجوز رفض الإنابة القضائية، دون تعليل، من قبل الجهة التي ترفضها.

المادة الواحدة والأربعون:

تلتزم كل من الدول المتعاقدة، بتنفيذ الإنابات القضائية، المتعلقة بالجرائم السيبرانية، ويجوز لها، رفض طلب التنفيذ، في أي من الحالتين الآتيتين:

أ. إذا كانت الجريمة، موضوع الطلب، محل اتهام، أو تحقيق، أو محاكمة، لدى الدولة المطلوب إليها، تنفيذ الإنابة.

ب. إذا كان تنفيذ الطلب، من شأنه المساس بسيادة الدولة المكلفة بتنفيذه، أو بأمنها، أو بالنظام العام فيها.

المادة الثانية والأربعون:

ينفذ طلب الإنابة، وفقا لأحكام القانون الداخلي، للدولة المطلوب إليها التنفيذ، وعلى وجه السرعة، ويجوز لهذه الدولة، تأجيل التنفيذ، حتى استكمال إجراءات التحقيق، والملاحقة القضائية، الجارية لديها، في الموضوع نفسه، أو زوال الأسباب القهرية، التي دعت للتأجيل، على أن يتم إشعار الدولة الطالبة، بهذا التأجيل.

المادة الثالثة والأربعون:

يكون للإجراء، الذي يتم بطريق الإنابة، وفقا لأحكام هذه الاتفاقية، الأثر القانوني ذاته، كما لو تم أمام الجهة المختصة، لدى الدولة طالبة الإنابة. على أنه، لا يجوز استعمال ما نتج عن تنفيذ الإنابة، إلا في نطاق ما صدرت الإنابة بشأنه.

١٢ . هيكلية ادارية لمتابعة شؤون الأمن السيبراني

المادة الرابعة والأربعون:

تتعهد الدول الأعضاء، اعتماد التدابير اللازمة لإنشاء هيكلية ادارية وطنية، متخصصة في متابعة الأمن والسلامة، في الفضاء السيبراني.

ويشكل إنشاء الهيكلية هذه، تعبيرا عن التزام الدولة الجدي، عبر كل مكوناتها الادارية، والمؤسساتية، بتأمين الثقة في الاقتصاد الرقمي، وحماية الفضاء السيبراني، ضمن إطار محدد، لقيادة واضحة وقوية، تتيح اتخاذ ما يلزم من تدابير، لتحقيق الآتي:

- تحديد المسؤولية، عن سلامة الفضاء السيبراني، وأمنه، على كل المستويات الحكومية، من خلال تحديد واضح، للمهام والادوار.
- تشجيع القطاع الخاص، على الانخراط في المبادرات الحكومية، الهادفة إلى حماية الفضاء السيبراني، وتعزيز الاقتصاد الرقمي.
- تكوين إدارة وطنية موسعة، متعددة الاختصاصات، خاصة بالأمن السيبراني، تضم خبراء واختصاصين، من المجالات كافة، بحيث تتمكن من رفع التحديات، التي تطرحها الأخطار السيبرانية، ومن التعامل، بفاعلية وسرعة، مع المستجدات، والطوارئ التي يمكن ان تحصل.

المادة الخامسة والأربعون:

تتخذ كل دولة عضو، ما تراه مناسبا من إجراءات، تمكنها من إنشاء مؤسسات، ذات كفاءة عالية لمكافحة الجريمة السيبرانية، ولنشر الوعي، وتحسيس المجتمع، والرد على طوارئ الانترنت، والتعامل مع الانذارات المبكرة الخاصة، بوجود مخاطر داهمة أو محتملة، وتولي التنسيق بين الجهات الوطنية المعنية بالأمن السيبراني، ومع الجهات الاقليمية والعربية والدولية، متى استدعى الامر ذلك. ويمكن في هذا المجال، إنشاء الهيئات الآتية، أو ما يشبهها:

- مجلس وطني للأمن والسلامة السيبرانية
- مركز استجابة لطوارئ الانترنت
- هيئة وطنية للسلامة والأمن، في المجال السيبراني، بهدف متابعة وتنفيذ، سياسة حماية وأمن وطنية، وتسهيل التعاون والتنسيق، على المستويين الداخلي والخارجي.
- هيئة وطنية لحماية البيانات الشخصية

المادة السادسة والأربعون:

تنشئ كل دولة، مجلسا وطنيا مستقلا، للسلامة والأمن في الفضاء السيبراني، يشكل المرجع الاعلى، لمسائل السلامة والأمن، في المجال السيبراني، وتكون مهامه:

- وضع استراتيجية سيبرانية، وسياسات تنفيذها
- الموافقة على الاستراتيجية والسياسة والموضوعتين في كل إدارة حكومية، لتنفيذها.
- تحديد اولويات الأمن، والمبادرات الوطنية
- تنسيق الجهود والمبادرات، على المستوى الوطني
- تحديد الجهات المعنية، والمولجة حفظ الأمن والسلامة، وارساء قواعد الثقة، في الاقتصاد الرقمي
- تنسيق العلاقات مع القطاع الخاص، لمعالجة مسائل الأمن والسلامة
- التعاون مع الأجهزة الأمنية المختلفة، مثل: المخابرات، والأمن العام، والأمن الداخلي، والشرطة القضائية، والجهات القضائية المعنية، بهدف وضع معايير واصول ردع وملاحقة وتحقيق موحدة، وإقرار توافق مؤسساتي
- التعاون مع الهيئات المسؤولة، عن تطبيق القانون، على المستويات الوطنية، الاقليمية والدولية.
- مراقبة انظمة المعلومات الحكومية، والبنية التحتية للاتصالات
- الاشراف على تطوير انظمة المعلومات، الخاصة بالهوية الرقمية، والهوية الرقمية الموحدة، وإدارة الممارسات في هذا المجال، واصدار التوصيات
- تطوير وتنسيق الجهود الخاصة، ببرامج تأهيل، وتدريب، وبناء قدرات، في مجال الأمن والسلامة في الفضاء السيبراني، والتعاون مع الجهات الوطنية، والاقليمية، والعربية، والدولية المعنية.

المادة السابعة والأربعون:

يتألف المجلس الوطني للسلامة والأمن، من الوزراء المعنيين: وزير الدفاع، وزير الداخلية، وزير الاتصالات، وزير الاقتصاد.

المادة الثامنة والأربعون:

إنشاء هيئة وطنية عليا مستقلة، للسلامة والأمن في المجال السيبراني، تضطلع بتنفيذ استراتيجيات وسياسات الأمن والسلامة، وبتنسيق الجهود الوطنية، في هذا المجال، وتتولى هذه السلطة:

- اتخاذ الخطوات التي تضمن تنفيذ التدابير، التي يحددها ويوصي بها، المجلس الوطني
- مراقبة التزام الجهات الحكومية، والخاصة، بما يوصي به المجلس الوطني
- الاشراف على اعمال تقييم مستوى السلامة والأمن، واعمال الخبرة Audit والتدقيق
- مساعدة المجلس الوطني، في عملياته التنفيذية.

- المشاركة في وضع القواعد، واعتماد المعايير والمقاييس الدولية، التي تضمن أمن الأنظمة المعلوماتية والمعلومات، وسلامة الاقتصاد الرقمي، والمصادقة على التوقيع الإلكتروني.
- مراقبة العقود، التي تبرمها الدولة، مع متعهدي الخدمات، وجميع المستثمرين، في مجال تقنيات المعلومات والاتصالات، الذين يقدمون خدمات، تتعلق باستخدام تقنيات المعلومات والاتصالات.

المادة التاسعة والأربعون:

تتألف الهيئة الوطنية العليا، من ممثلين عن الأجهزة المعنية بتنفيذ السياسات، وحفظ الأمن.

المادة الخمسون:

تتعهد الدول المتعاقدة، إنشاء مراكز الاستجابة لطوارئ الانترنت، تكون مسؤولة عن مراقبة وحماية البنية التحتية للمعلومات والاتصالات، من الاعتداءات عليها، وتشكيل نقطة اتصال وتنسيق وطنية، يمكنها ان تتجاوب ومتطلبات الرد السريع، على الأخطار السيبرانية، على المستويات الوطنية والاقليمية والعربية والدولية وتضمن الدولة:

- أهلية مراكز الاستجابة لطوارئ الانترنت، على العمل بطريقة احترازية وردعية، وتأمين توزيع المعلومات، حول الطوارئ على الانترنت، في الوقت المناسب، للحماية منها، أو للحد من اضرارها، والقدرة على المساعدة في مواجهة الأخطار، ومعالجة نتائج الاعتداءات بطريقة سريعة وفاعلة.
- تولي المراكز، انذار المؤسسات والادارات والأفراد، وتحصين أنظمة المعلومات، ومعالجة الحوادث، وتنظيم وتنسيق جهود الرد، على الهجمات والاعتداءات، ومعالجة نقاط الضعف، ومشاكل الابواب الخلفية، ودراستها وتحليلها، واستنباط الحلول الملائمة.
- تولي المراكز، مهمة الإعلام والإعلان، عن الطوارئ، والمخاطر، والحوادث، وتقديم خدمات الخبرة، والتدقيق في مدى جهوزية الأنظمة، وقدرتها على مواجهة الأخطار، ورد الهجمات والاعتداءات، وتطوير برامج حماية، وتوفير خدمات رصد الهجمات والاعتداءات، ومنع وقوعها.
- رصد، وتحليل، وتنسيق الجهود، في مواجهة الفيروسات، والبرامج التجسسية والخبيثة، ودراسة المخاطر، وتحليلها، ومتابعة، ومواكبة اعادة الأنظمة المعلوماتية، إلى ما كانت عليه، وتقديم استشارات في مجال الحماية، وأمن الأنظمة، والشبكات والمعلومات.
- تنظيم حملات توعية، والمصادقة على اعمال الخبرة، والتدقيق، وشهادات الكفاءة، في مجال أمن الاتصالات.
- التعاون الوثيق، بين المراكز الوطنية، ومراكز الاستجابة لطوارئ الانترنت، الدولية والاقليمية، كما يكون من الافضل، ان تنتسب، إلى الشبكات الدولية، لمراكز الاستجابة لطوارئ الانترنت.

١٣. الإطار التشريعي لبناء الثقة في الفضاء السيبراني

المادة الواحدة والخمسون:

تتعهد كل دولة متعاقدة، إقرار اطر تشريعية وتنظيمية، استنادا إلى النصوص الدولية، والاتفاقيات، وبروتوكولات التعاون، الصادرة حول بناء الثقة في الفضاء، لاسيما منها تلك الخاصة، بمكافحة الجريمة السيبرانية، والتعاون في الجرائم العابرة للحدود، والمقاييس والمعايير الدولية، المفروض اعتمادها، في حماية البنية التحتية للاتصالات، وانظمة المعلومات، لاسيما منها على سبيل المثال: القرارات الصادرة عن الجمعية العامة للامم المتحدة، ٤٥/١٢١، و ٥٥/٦٣، و ٥٦/١٢١، و ٦٠/١٧٧، والقوانين النموذجية الخاصة بالجريمة السيبرانية، وحماية الفضاء السيبراني، لاسيما نها، ما اعتمدته جامعة الدول العربية، ومجلس وزراء العدل العرب، أو مجلس وزراء الاتصالات العرب، والقانون الصادر في إطار دول الكومنولث، والاتفاقيات الأوروبية حول الجريمة السيبرانية، وحماية البيانات الشخصية، وبيانات الاتصال، وإعلان سلفادور، الذي اعتمده مؤتمر الأمم المتحدة، عام ٢٠١٠.

المادة الثانية والخمسون:

تلتزم الدول الأعضاء، إقرار التشريعات الملائمة لتشجيع الانخراط السليم والأمن، في مجتمع المعلومات، والافادة من آفاق مجتمع المعرفة، بما يخدم النمو والتنمية، لاسيما فيما يتعلق ب:

- تنظيم التجارة الإلكترونية
- حماية الخصوصية والحق في التعبير
- ضمان الحق في النفاذ إلى الشبكة العالمية للمعلومات
- حماية البيانات الشخصية، والبيانات الحساسة
- تنظيم المحتوى
- حماية الملكية الفكرية والصناعية، وحقوق المؤلف، والحقوق المجاورة
- حماية الاطفال على الانترنت
- تنظيم المعاملات الإلكترونية
- تنظيم المسؤوليات، وخدمات الحوسبة السحابية
- إقرار قواعد تجريم موضوعية
- إقرار تشريعات خاصة بمكافحة الجرائم السيبرانية
- وضع أصول ملاحقة، ومتابعة، وتنفيذ، خاصة بالجرائم السيبرانية
- إقرار آليات تعاون وطنية، واقليمية، ودولية
- لحظ هيكلية ادارية خاصة، لحماية الفضاء السيبراني
- إقرار الإطار التشريعي الملائم، للتعاون بين القطاعين العام والخاص، في مواجهة الجرائم السيبرانية

المادة الثالثة والخمسون:

تتعهد كل دولة متعاقدة، ضمان انسجام الإجراءات والقواعد القانونية التي تتخذها، في مجال مكافحة الجريمة السيبرانية، مع أفضل النصوص الدولية، المعمول بها في هذا المجال، ومع الممارسات الفضلى، مع الاخذ بعين الاعتبار، الحد الادنى المعتمد في الدول، التي لديها أدوات تشريعية وتنظيمية، بحيث يكون المجال متاحا، أمام امكانية تحقيق الانسجام، بين تشريعات الدول الأعضاء.

المادة الرابعة والخمسون:

تعتمد الدول الأعضاء، فيما يتعلق بالجرائم العابرة للحدود، على مبدأ توحيد القواعد القانونية، الخاصة بتجريم الأعمال الجرمية السيبرانية، واصول الملاحقة والتنفيذ، الخاصة بها، بحيث تعتمد كل دولة، القواعد القانونية، التي تسمح لها باعتماد مبدأ التجريم المزدوج، وذلك بهدف انجاح التعاون، وتفعيله.

المادة الخامسة والخمسون:

تقر الدول الأعضاء، القواعد القانونية والتنظيمية، التي تراها ضرورية، والتي تنسجم مع تشريعاتها الوطنية، لتسهيل عملية تبادل المعلومات، وتشارك البيانات، بشكل سريع، فوري ومتبادل بين الهيئات المتخصصة، وذات الصلاحية في تطبيق القوانين، في الدول الأعضاء.

المادة السادسة والخمسون:

تعمد الدول الأعضاء، إلى مراجعة تشريعاتها، بهدف التأكد من فعاليتها، في تجريم، ومعاقبة، كل اشكال اساءة استخدام تقنيات المعلومات والاتصالات، بالشكل المناسب، ومن قدرتها على رفع التحديات ذات العلاقة بالصلاحية، والاختصاص القضائي، ووسائل التحقيق والملاحقة، والتكوين، والتدريب، والحماية من الجرائم السيبرانية، والتعاون الدولي في هذا المجال.

وتلتزم الدول، في هذا السياق، السعي إلى الانسجام، مع توصيات وتوجيهات، المنظمة العربية لحماية الفضاء السيبراني، والمقررات الدولية، التي تصدر، لاسيما:

- مقررات وتوصيات الأمم المتحدة ولجانها المختصة، بمكافحة الجرائم السيبرانية، والجرائم العابرة للحدود.
- توجيهات الاتحاد الدولي للاتصالات، لاسيما منها، ما يتعلق بسبل وآليات، تحقيق الأمن السيبراني
- الاتفاقات الجماعية والثنائية، التي تلتزم بها، في مجال مكافحة الجرائم العابرة للحدود.
- الاتفاقيات والمعاهدات الدولية، الخاصة بحماية الملكية الفكرية، وحماية البيانات الشخصية، ومكافحة الجريمة السيبرانية.

المادة السابعة والخمسون:

في إطار مكافحة الجريمة السيبرانية، وتفعيل سلطاتها القضائية والعسكرية، والاستخباراتية، والأمنية، ومحافظتها على الأمن القومي، والمصلحة العامة، وقيمها الاجتماعية والثقافية، تلتزم الدول الأعضاء، العمل على إيجاد الآليات القانونية، التي تنسجم مع تشريعاتها الوطنية، للحفاظ على الحق في الخصوصية، وعلى حماية الحياة الشخصية والحريات، سواء على المستوى الوطني، أو على مستوى التعاون الاقليمي والدولي.

المادة الثامنة والخمسون:

تتعهد الدول الأعضاء، بمكافحة جميع أنواع جرائم الاستغلال الجنسي للاطفال، باستخدام تقنيات الاتصالات والمعلومات، وبوضع الاطر التشريعية والتنظيمية الملائمة، للتعاون الفاعل، التي تجرم هذه الأعمال، عبر تمكين السلطات المعنية بالمكافحة، والبحث والملاحقة، ووضع برامج تربوية مناسبة، وإنشاء قواعد خاصة بالاستغلال الجنسي للاطفال، وتوفير خط ساخن للشكاوى والاستعلام، والتعاون مع القطاع الخاص، والمجتمع المدني، ومتعهدي الخدمات، لاستنباط السبل الامثل، للمكافحة والتوعية.

١٤ . التجارة الإلكترونية

المادة التاسعة والخمسون:

تلتزم الدول المتعاقدة، توفير المستلزمات الضرورية، لممارسة التجارة الإلكترونية، بحرية تامة. كما تتعهد الدول المتعاقدة، الزام ممارسي التجارة الإلكترونية، مراعاة مصالح المستهلك، وضمان حقه في التحقق من هوية مقدمي الخدمات، عبر الإعلان الواضح، عن الاسم للشخص الطبيعي أو المعنوي، ومحل اقامته، وعنوانه الكامل، وأرقام الهاتف، وكيفية الاتصال به، ومعلومات حول وضعه المهني، كالتسجيل في نقابة، أو سجل تجاري، ورقم التسجيل، ورأس المال، واجازة ممارسة العمل التجاري، وشروط المهنة التي ينتمي اليها، والبلد، والجنسية. يضاف إلى هذا، ضرورة إقرار مسؤوليته عن تنفيذ التزاماته، سواء أكان المنفذ المباشر للخدمة، أو بالواسطة.

المادة الستون:

تحظر ألعاب الميسر، والحظ، ولو كانت بشكل العاب لوتو، أو مراهنات، كما تحظر الخدمات القانونية، والطبية، باستخدام تقنيات المعلومات والاتصالات.

المادة الواحدة والستون:

تتعهد الدول المتعاقدة، باتخاذ الإجراءات التشريعية اللازمة، لتنظيم الإعلان التجاري، الذي تستخدم فيه ارقام الهواتف، والعناوين الإلكترونية، لاسيما لجهة الزام المعلن، باحترام حق كل مستهدف بالإعلان، في رفض تلقي رسائل، أو اتصالات إعلانية.

المادة الثانية والستون:

تتعهد الدول المتعاقدة، باتخاذ الإجراءات التشريعية اللازمة، لتأمين إطار قانوني، خاص يعترف بالعقود الإلكترونية، واثباتها، ومفاعلها، وكيفية انعقادها، وآليات الإعلان عن القبول.

كما تتعهد، باتخاذ الإجراءات التشريعية اللازمة، لتأمين القوة الثبوتية، للاعتراف بالسند الإلكتروني، وحجية التحويلات الإلكترونية، من خلال تنظيم التوقيع الإلكتروني.

١٥ . حماية البيانات الشخصية

المادة الثالثة والستون:

على كل دولة، ان تتخذ الإجراءات التشريعية والتنظيمية المناسبة، لحماية البيانات الشخصية، بما يمنع الاعتداء على الحياة الشخصية، والذي يمكن ان ينتج، عن معالجة البيانات، وجمعها، ونقلها، واستثمارها، وتخزينها، واستخدامها.

ويفترض بالتشريع، ان يراعي الحريات الشخصية، والحقوق الأساسية للانسان، مع الحفاظ على صلاحيات الدولة، وحقوق الهيئات المحلية، ومصالح الشركات والمؤسسات، التي تتعاطى مع البيانات.

المادة الرابعة والستون:

يتناول التشريع والتنظيم، كل معالجة إلكترونية، أو غيرها، ونقل، وتخزين، واستخدام، للبيانات الشخصية، سواء من قبل الاشخاص الطبيعيين، أو الدولة، أو الشركات والمؤسسات، أو الهيئات المحلية، أو الاشخاص الطبيعيين، بشكل عام.

المادة الخامسة والستون:

لا يدخل في نطاق هذه الحماية:

- البيانات الخاصة بالسلامة العامة، والدفاع، والبحث والتحري عن الجرائم، وأمن الدولة، وذلك مع مراعاة النصوص القانونية المرعية الإجراء، لدى الدولة.
- معالجة البيانات، التي يقوم بها أشخاص طبيعيون، في إطار نشاطهم الشخصي، أو المحلي، شرط الا يكون هدف المعالجة، نقل البيانات إلى الاشخاص الثالثين، أو النشر.
- النسخ التقنية، التي تستهدف تسهيل عمليات البحث، على الأنظمة المعلوماتية

المادة السادسة والستون:

تشترط الدول المتعاقدة، التزام الجهة الراغبة بمعالجة البيانات الشخصية، أو تخزينها، أو نقلها، أو استعمالها، الحصول على اذن مسبق، من الهيئة الوطنية المسؤولة عن حماية البيانات، والالتزام بالشروط التي تضعها، هذه الهيئة.

المادة السابعة والستون:

تتولى الهيئة الوطنية، وضع الشروط المناسبة، لحماية البيانات الشخصية، والحياة الخاصة، بحسب الإطار التشريعي والتنظيمي الوطني، الذي يرعى الموضوع، وبحسب القوانين المرعية الإجراء.

وتضع الهيئة المعايير المناسبة، كما تحدد البيانات الشخصية المستثناة، وظروف الاستثناء، اضافة إلى المدة القصوى للاحتفاظ بالبيانات، وكيفية حمايتها، ومنع تسربها، واصول نقلها إلى دول أخرى، أو أشخاص طبيعيين، في القطاعين: العام أو الخاص.

وتلتزم الهيئة الوطنية بالرد، في مهل تحدد بالقانون، وبتعليل قرارها، في حال الرفض.

المادة الثامنة والستون:

تتألف الهيئة الوطنية لحماية المعلومات، كإدارة مستقلة، وتضم أعضاء من البرلمانيين، والأكاديميين، والخبراء، والتقنين، والمجتمع المدني، والهيئات الاقتصادية. ويتمتع أعضاء الهيئة بحصانة، تمنع التعرض لهم، بسبب القرارات التي تتخذها الهيئة.

١٦ . تجريم الاعتداء على البيانات والأنظمة المعلوماتية

المادة التاسعة والستون:

تتعهد الدول المتعاقدة، تجريم الأعمال، التي تستهدف سرية الأنظمة المعلوماتية، والبيانات الإلكترونية، ومصداقيتها، وتوفرها، وانسيابها الحر.

المادة السبعون:

تتخذ كل دولة، الإجراءات التشريعية الضرورية بحسب نظامها، وقوانينها الوضعية، لتجريم اختراق الأنظمة المعلوماتية، والدخول قصدا، إلى نظام معلوماتي، أو إلى جزء منه، دون وجه حق، أو دون اذن، من الجهة صاحبة الصلاحية في الاذن بذلك، سواء عبر الالتفاف على الإجراءات الأمنية المعتمدة، أو عبر النفاذ من خلال جهاز موصول إلى النظام، بقصد سرقة البيانات، أو الاطلاع عليها، أو تحويرها، أو لاي هدف آخر، غير قانوني.

المادة الواحدة والسبعون:

تتخذ كل دولة، الإجراءات التشريعية الضرورية، بحسب نظامها، وقوانينها الوضعية، لتجريم اعتراض انسياب البيانات، وانتقالها، قصدا، ودون وجه حق، من والى اي نظام معلوماتي، أو جهاز كومبيوتر، بغض النظر عن تقنية النقل، أو الانسياب. ويمكن للدولة، اشتراط توفر سوء النية.

المادة الثانية والسبعون:

تتخذ كل دولة، الإجراءات التشريعية الضرورية، بحسب نظامها، وقوانينها الوضعية، لتجريم العبث بالمعلومات عن قصد، ودون وجه حق، لاتلاف البيانات، أو محوها، أو تخريبها، أو تحويرها، أو تعديلها. ويمكن للدولة المعنية، اشتراط حصول ضرر، لإقرار حصول الجرم.

المادة الثالثة والسبعون:

تتخذ كل دولة، الإجراءات التشريعية الضرورية، بحسب نظامها، وقوانينها الوضعية، لتجريم العبث بالنظام المعلوماتي عن قصد، ودون وجه حق، لاعاقة عمل النظام، سواء عبر ادخال بيانات إلكترونية، أو نقلها، أو ارسالها، أو الحاق الضرر بها، أو محوها، أو تحويرها، أو تعديلها.

المادة الرابعة والسبعون:

تتخذ كل دولة، الإجراءات التشريعية الضرورية، بحسب نظامها، وقوانينها الوضعية، لتجريم الافعال التالية، عندما ترتكب عن قصد، ودون وجه حق، تصنيع، انتاج، بيع، الاستيلاء بقصد الاستعمال، استيراد، توزيع أو توفير:

- أدوات، بما فيها البرامج المعلوماتية، معدة لارتكاب أي من الأعمال الجرمية، المذكورة في المواد السابقة
- كلمات سر، رمز دخول، أو اي بيانات مشابهة، يمكن من خلالها الوصول إلى نظام معلوماتي، أو إلى جزء منه، بهدف ارتكاب اي من الأعمال الجرمية، المذكورة في المواد السابقة
- حيازة أدوات، بما فيها البرامج المعلوماتية، وكلمات السر، ورمز الدخول، أو اي بيانات تساعد على اقتحام نظام معلوماتي، أو جزء منه.

لا تطبق هذه المادة، على الافعال المذكورة فيها، متى كان الهدف منها، إجراء اختبارات، لتقييم مستوى الأمن في الأنظمة المعلوماتية المستهدفة، شرط ان تتم هذه الاختبارات، بناء على اذن مسبق، من الجهة صاحبة الصلاحية.

المادة الخامسة والسبعون:

تتخذ كل دولة، الإجراءات التشريعية الضرورية، بحسب نظامها، وقوانينها الوضعية، لتجريم ادخال البيانات، أو تشويهها، أو تعديلها، أو محوها، متى ارتكبت عن قصد، ودون وجه حق، بنية جعل هذه البيانات، تبدو أصلية وصحيحة، وبهدف استخدامها، لاسباب قانونية، كالاثبات، بغض النظر عما اذا كانت البيانات، مرمزة، أو مشفرة، أو مقروؤة أو مفهومة. ويمكن للدولة المعنية، اشتراط نية الخداع، أو الاحتيال، أو غيرها من سوء النية، لتقرير المسؤولية الجزائية.

المادة السادسة والسبعون:

تتخذ كل دولة، الإجراءات التشريعية الضرورية، بحسب نظامها، وقوانينها الوضعية، لتجريم الافعال التالية، متى ارتكبت عن قصد، ودون وجه حق، ومتى تسببت في خسارة ملكية، عائدة لاحد الاشخاص:

- اي ادخال أو تعديل، أو تحوير، أو محو، أو اخفاء، لبيانات إلكترونية
- أي تدخل في عمل النظام المعلوماتي، دون وجه حق، وعن سوء نية، أو بهدف الغش، للحصول على مكتسبات اقتصادية، لحساب منفذ التدخل نفسه، أو لحساب شخص آخر

المادة السابعة والسبعون:

تتعهد الدول، تأمين حماية فاعلة للاطفال، في الفضاء السيبراني، وعلى مختلف وسائل الاتصالات.

وتحقيقا لهذه الغاية، تتخذ كل دولة، الإجراءات التشريعية الضرورية، بحسب نظامها، وقوانينها الوضعية، لتجريم الافعال التالية، عندما تكون مرتكبة عن قصد، ودون وجه حق:

- انتاج مواد إباحية، تستخدم الاطفال، بهدف توزيعها، عبر أنظمة معلوماتية
- عرض مواد اباحية، تستخدم الاطفال، أو توزيعها، عبر أنظمة معلوماتية
- توزيع، أو نقل، أو بث، مواد اباحية، تستخدم الاطفال، عبر أنظمة معلوماتية
- الحصول على مواد اباحية تستخدم الاطفال، عبر أنظمة معلوماتية، للاستعمال الشخصي، أو لصالح شخص آخر
- حيازة مواد اباحية، تستخدم الاطفال، على أنظمة معلوماتية، أو على أي جهاز، أو وسيلة، يمكن حفظ البيانات الإلكترونية عليها

والمواد الاباحية، التي تستخدم الاطفال، هي كل مادة مرئية، تظهر قاصرا في فعل جنسي ظاهر، أو تظهر شخصا يبدو قاصرا، في فعل جنسي ظاهر، أو صورا واقعية، تمثل قاصرا، يمارس نشاطا جنسيا ظاهرا.

ويعتبر قاصرا، لتطبيق هذه الاحكام، أي شخص، لم يبلغ الثامنة عشرة من عمره، ولا يمكن تخفيض سن البلوغ، إلى أقل من ستة عشر عاما.

المادة الثامنة والسبعون:

تتخذ كل دولة، الإجراءات التشريعية الضرورية، بحسب نظامها، وقوانينها الوضعية، لتجريم الافعال، التي تشكل اعتداء على حقوق الملكية الفكرية، والصناعية، وحقوق المؤلف، والحقوق المجاورة، بحسب ما تنص عليه قوانينها الوضعية، وبما ينسجم مع المعاهدات الدولية، التي تكون قد انضمت اليها، كلما كانت هذه الافعال، قد ارتكبت عن قصد، وبهدف الافادة المادية، والاتجار بالمواد التي تمت قرصنتها، عبر استخدام الأنظمة المعلوماتية.

المادة التاسعة والسبعون:

تتخذ كل دولة، الإجراءات التشريعية الضرورية، بحسب نظامها، وقوانينها الوضعية، لتجريم الافعال التي تشكل تدخلا، أو شروعا، أو مساعدة، أو تحريضا، على ارتكاب الجرائم السيبرانية، الواردة في هذه الاتفاقية.

المادة الثمانون:

تتخذ كل دولة، الإجراءات التشريعية الضرورية، بحسب نظامها، وقوانينها الوضعية، لإعلان مسؤولية الاشخاص المعنويين، الجزائية، أو المدنية، أو الادارية، عن الأعمال الجرمية، الواردة في هذه الاتفاقية، والتي يتم ارتكابها، من قبل الأفراد الطبيعيين لمصلحتهم، سواء أعملوا منفردين، أو كجزء من أحدى هيئات الشخص المعنوي، ذات المركز القيادي، ومتى كان لمرتكب الافعال:

- الصفة القانونية، لتمثيل الشخص المعنوي
- السلطة لاتخاذ قرارات، لصالح الشخص المعنوي
- السلطة للرقابة والاشراف

لا يؤثر إعلان مسؤولية الشخص المعنوي الجزائية، على المسؤولية الجزائية للشخص الطبيعي، مرتكب الجرم.

المادة الواحدة والثمانون:

تحرص الدول المتعاقدة، على اتخاذ الإجراءات التشريعية الضرورية، بحسب نظامها، وقوانينها الوضعية، التي تكفل تجريم الافعال، التي تهدد الأمن السيبراني، لاسيما منها الجرائم المذكورة في هذه الاتفاقية، بعقوبات رادعة، وفاعلة، تتناسب مع خطورتها، وعلى ان تلحظ عقوبة السجن، بالنسبة للافراد الطبيعيين، والجزاءات المالية الرادعة، والمناسبة، بالنسبة للاشخاص المعنويين.

١٧. المنظمة العربية لحماية الفضاء السيبراني

المادة الثانية والثمانون:

تنشأ بموجب هذه الاتفاقية، منظمة خاصة، اسمها: المنظمة العربية للفضاء السيبراني.

المادة الثالثة والثمانون:

تتولى المنظمة العربية، لحماية الفضاء السيبراني:

- مواكبة التطورات الحاصلة، على مستوى تقنيات الاتصال والمعلومات
- وضع توصيات، وإقرار معايير، واعتماد ممارسات فضلى، خاصة بحماية البنية التحتية، وسلامتها
- اقتراح القواعد التنظيمية المناسبة، لضبط الأمن والسلامة، في الفضاء السيبراني
- وضع آلية خاصة، لتبادل البيانات، والمعلومات، بين الأجهزة المعنية، بتطبيق القانون والملاحقة، في كل دولة.
- الاشراف على إنشاء شبكة عربية، لمراكز طوارئ الانترنت، تشكل إطار التعاون فيما بينها، والتنسيق مع المراكز الدولية المشابهة، والمؤسسات الأمنية الاخرى، التي تمارس نشاطا متصلا، أو متمما لنشاطها.

- اقتراح، ووضع الاطر المناسبة لتبادل المعلومات والخبرات، بين الأجهزة القضائية والأمنية العربية، المعنية بمكافحة الجرائم السيبرانية، وحماية سلامة وأمن الفضاء السيبراني
- اعتماد وتعديل، المعايير، والممارسات المعتمدة، ومتابعة تطوير إجراءات التعامل مع كافة المسائل الخاصة بالسلامة والأمن في الفضاء السيبراني
- وضع قوانين نموذجية، تنظم المسائل المتصلة، ببناء الثقة في الفضاء السيبراني، ومجتمع المعلومات والمعرفة، مثل: التجارة الإلكترونية، أمن البيانات، أمن الأنظمة المعلوماتية، حماية البيانات الشخصية، تنظيم المحتوى غير المشروع والمحتوى المؤذي، التوقيع الإلكتروني ، خدمات المصادقة على التواقيع، التحقيقات الجزائية والملاحقات، التتبع والرصد والاثبات، تطبيقات الحكومة الإلكترونية، حماية الخصوصية وحرية المعلومات، في قطاع الاتصالات الإلكترونية، حقوق الملكية الفكرية والصناعية، والحقوق المجاورة أمن المعاملات الإلكترونية، حماية الاطفال على الانترنت، الخ....

المادة الرابعة والثمانون:

تعتبر الدول العربية، الأعضاء في الاتفاقية، أعضاء، في المنظمة العربية للفضاء السيبراني.

المادة الخامسة والثمانون:

تتألف المنظمة من: الهيئة العامة، التي تضم ممثلين عن جميع الدول الأعضاء، ومن الهيئة التنفيذية، ومن المجلس الاستشاري العربي، لشؤون الأمن السيبراني.

المادة السادسة والثمانون:

تعين الهيئة العامة، أعضاء الهيئة التنفيذية، بناء على ترشيحات، تتقدم بها الدول الأعضاء.

المادة السابعة والثمانون:

تتولى الهيئة التنفيذية، اعمال اليومية لإدارة المنظمة، ويرأسها امين عام، يمثل المنظمة أمام المحافل الدولية، ولدى الدول الأعضاء، وأمام المحاكم.

المادة الثامنة والثمانون:

يعاون الهيئة التنفيذية، لجنة تقنية، ولجنة قانونية، ولجنة التعاون والدبلوماسية، ولجنة التحقيقات والملاحقة. ويمكن للهيئة العامة ان تقر إنشاء لجان أخرى، فيما لو اقتضت ضرورات العمل ذلك.

المادة التاسعة والثمانون:

ينشأ مجلس استشاري، يدعى «المجلس الاستشاري العربي لشؤون الأمن السيبراني»، وتنشأ لجان متخصصة، لمعاونة الهيئة العامة، والهيئة التنفيذية، على ضوء حاجات تسيير العمل في المنظمة.

المادة التسعون:

يتكون المجلس الاستشاري العربي، من ٧ أعضاء، يتم ترشيحهم من قبل الدول الأعضاء، انطلاقا، من لائحة من الخبراء المشهود لهم، بالكفاءة العالية في مجال الأمن السيبراني، ويجري انتخابهم من قبل أعضاء المنظمة العربية لحماية الفضاء السيبراني. يتولى المجلس الاستشاري القضايا الآتية:

- تعزيز نشر الوعي في العالم العربي، حول أهمية الأمن السيبراني، وضرورة حماية الحريات، والحقوق الشخصية والمدنية، على الانترنت
- تشجيع الاعتماد، على تقنيات الحماية، والمعايير الدولية، في حماية الأنظمة
- نشر ثقافة الأمن السيبراني، عبر تنظيم نشاطات، ثقافية وإعلامية
- إنشاء قواعد معلومات، خاصة بالجرائم السيبرانية، وآثارها، وانعكاساتها السلبية
- تحديد الحاجات، والتحديات، والأخطار، والأولويات في مجال الأمن السيبراني، على المستوى العربي، وتحديد أفضل السبل والأساليب، للتعاون على مواجهتها
- تحليل، ودراسة الظواهر، المرتبطة بأمن الفضاء السيبراني
- اعطاء الاستشارات للدول، حول كيفية وضع، استراتيجيات وسياسات الأمن السيبراني، ومكافحة الجريمة السيبرانية، وضمان السلامة، في الفضاء السيبراني
- اعداد دراسات، حول السلوكيات المسيئة والجرمية، للمستخدمين، والمجرمين، والأنظمة المعلوماتية
- وضع أدلة استرشادية، حول الممارسات الفضلى، ومستويات الخطر، والانعكاسات السلبية، للجرائم السيبرانية
- وضع تقارير دورية، حول واقع الأمن السيبراني، في الدول العربية، والخطوات التي تحققها كل دولة عضو، على مستوى تنفيذ الاتفاقية، واحترام مندرجاتها، ورفعها إلى المنظمة العربية، لحماية الفضاء السيبراني
- التعاون مع الهيئات الوطنية، في مجال حماية الفضاء السيبراني

المادة الواحدة والتسعون:

تتولى الهيئة العامة، وضع النظام الداخلي، لكل هيئة تنشئها، وذلك في غضون شهر من تاريخ تأليفها.

١٨. احكام ختامية

المادة الثانية والتسعون:

يمكن لأي دولة عربية، طلب الانضمام إلى هذه الاتفاقية، سواء عبر توقيعها، أو الانضمام اليها. ولا تنفذ هذه الاتفاقية، بحق أية دولة عربية، إلا بعد إيداع وثيقة التصديق عليها، أو قبولها، أو إقرارها، لدى الأمانة العامة للمنظمة العربية لحماية الفضاء السيبراني، وبعد مضى ثلاثين يومًا من تاريخ الإيداع. وعلى الأمانة العامة، إبلاغ سائر الدول الأعضاء، بكل إيداع لتلك الوثائق، وتاريخه.

المادة الثالثة والتسعون:

تدخل هذه الاتفاقية حيز التنفيذ، بعد ثلاثين يوما، من توقيع عشر دول عربية عليها. وتعتبر نافذة على المستوى الوطني، بعد ثلاثين يوما، من موافقة السلطات المختصة بالتشريع، في الدولة المعنية.

المادة الرابعة والتسعون:

يمكن لكل دولة موقعة على الاتفاقية، ان تسجل تحفظاتها، شرط الا تتعارض هذه التحفظات، مع أهداف ومبادئ الاتفاقية، وشرط الا تؤثر على تطبيقها، بشكل فاعل.

المادة الخامسة والتسعون:

يمكن تعديل هذه الاتفاقية، بناء على طلب خطي، تتقدم به احدى الدول الأعضاء، إلى رئيس المنظمة العربية لحماية الفضاء السيبراني، الذي يبلغ الدول الأعضاء، ويدعوهم إلى دراسة التعديل المقترح، بعد مضي ثلاثة أشهر، على آخر تبليغ.

المادة السادسة والتسعون:

يمكن لأية دولة موقعة على الاتفاقية، أن تنسحب من هذه الاتفاقية، بناء على طلب خطي، ترسله إلى أمين عام المنظمة العربية لحماية الفضاء السيبراني، ولا يرتب الانسحاب أثره، الا بعد مضى ستة شهور من تاريخ إرسال الطلب، وتظل أحكام هذه الاتفاقية نافذة في شأن التعاملات، والطلبات، والدعاوى، التي قدمت قبل انقضاء هذه المدة.


جامعة الدول العربية - مجلس وزراء العدل العرب
المركز العربي للبحوث
القانونية والقضائية